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

Volume 88 (2019) Article 4

Text Message Privacy: Who Else Is Reading This?

Gerald Chan
Stockwoods LLP

Citation Information

Chan, Gerald. "Text Message Privacy: Who Else Is Reading This?." *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 88. (2019).
https://digitalcommons.osgoode.yorku.ca/sclr/vol88/iss1/4

Part III

Frontiers of Privacy

Text Message Privacy: Who Else Is Reading This?

Gerald Chan*

I. INTRODUCTION

Who talks on the phone anymore? Many of us perhaps. But we do so far less than we did 10 to 15 years ago. And we are increasingly relying on text conversations — whether through Short Message Service ("SMS") messaging, e-mail or some other "app" — as our primary mode of communication. A 2014 Gallup poll found that Americans under the age of 50 text more than they talk on their cell phones.[1] Canadians are unlikely to be much different, and the numbers have almost certainly moved further in the direction of texting over the last four years.

It is easy to see why texting has exploded in popularity. As a mode of communication, texting can be more efficient, allowing us to stretch out a series of conversations over a 16-hour work day without taking too much time from our daily checklist. Texting is also, in many ways, the most private form of communication. No one has any idea who we are communicating with (or if we are communicating at all) when we sit in the corner of a crowded room and tap away on our phones.

Of course, the law lags behind technology. Texting has been popular for over a decade, yet the Supreme Court of Canada did not address the issue of text message privacy until December 8, 2017, when it released *R. v. Marakah*[2] and *R. v. Jones.*[3] In these cases, the Court clarified the law on when the state can access our private text communications and the scope of our protections under section 8 of the *Charter of Rights and*

---

* Partner, Stockwoods LLP. The Author and his partner, Nader R. Hasan, were counsel to the British Columbia Civil Liberties Association, which intervened in *Marakah* and *Jones*. An abbreviated version of this chapter previously appeared on "Robichaud's Criminal Defence Litigation" blog ("Text Message Privacy: Where We Are and Where We Are Going") and The Advocates' Journal, Vol. 36, No. 4 (Spring 2018) ("Text messaging: The most private (and recorded) form of communication").

1 Frank Newport, "The New Era of Communication Among Americans" *Gallup* (November 10, 2014), online: <http://news.gallup.com/poll/179288/new-era-communication-americans.aspx>.

2 [2017] S.C.J. No. 59, 2017 SCC 59 (S.C.C.) [hereinafter "*Marakah*"].

3 [2017] S.C.J. No. 60, 2017 SCC 60 (S.C.C.) [hereinafter "*Jones*"].

Freedoms.[4] In *Marakah,* the majority held that both parties to a text conversation have a reasonable expectation of privacy in its contents regardless of the device the police search. In *Jones*, the Court clarified that the police require a production order to obtain historical text messages from a service provider such as TELUS, as opposed to a more rigorous Part VI[5] (wiretap) authorization when obtaining text messages on a prospective basis. These cases are summarized in this paper, along with an analysis of unresolved issues and the future Supreme Court cases that might address them.

II. JURISPRUDENTIAL CONTEXT

In the Charter, the right to privacy is protected by the section 8 right to be "secure against unreasonable search or seizure". The state conducts a "search", the courts have held, when it invades an area in which we have a "reasonable expectation of privacy".[6] This can occur when the state enters our physical spaces such as our homes (territorial privacy), inspects our bodies (bodily privacy), or obtains "personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state"[7] (informational privacy).[8] Where an individual's reasonable expectation of privacy has been invaded, she or he has standing to challenge the invasion as an unreasonable search or seizure under section 8 of the Charter and seek the remedy of exclusion of evidence under section 24(2).

Since 2009, the Supreme Court of Canada has applied these principles to the digital world in a series of cases. In *R. v. Morelli*,[9] *R. v. Cole*,[10] *R. v. Vu*[11] and *R. v. Fearon*,[12] the Court clarified the law on when police can search the contents of our digital devices (both personal and, in the case of *Cole,* workplace devices). In *R. v. Spencer*,[13] the Court looked at the reasonable expectation of privacy that we have in our online activities, as

---

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

5 *Criminal Code*, R.S.C. 1985, c. C-46.

6 *R. v. Tessling*, [2004] S.C.J. No 63, 2004 SCC 67, at para. 18 (S.C.C.).

7 *Id.*, at para. 25.

8 *Id.*, at paras. 22-24.

9 [2010] S.C.J. No. 8, 2010 SCC 8 (S.C.C.).

10 [2012] S.C.J. No. 53, 2012 SCC 53 (S.C.C.) [hereinafter "*Cole*"].

11 [2013] S.C.J. No. 60, 2013 SCC 60 (S.C.C.) [hereinafter "*Vu*"].

12 [2014] S.C.J. No. 77, 2014 SCC 77 (S.C.C.) [hereinafter "*Fearon*"].

13 [2014] S.C.J. No. 43, 2014 SCC 43 (S.C.C.) [hereinafter "*Spencer*"].

revealed by Internet service providers when they disclose to police the customer name and address information associated with a particular Internet protocol ("IP") address.

Until *Marakah*, however, the Court had not examined how section 8 of the Charter applies to text messaging as its own unique category of information. The closest it came was in *R. v. TELUS Communications Co.*,[14] when it interpreted the wiretapping regime in the *Criminal Code* (Part VI) to apply to the "interception" of text messages and not just phone calls. The Court reached this conclusion because Part VI speaks of intercepting "private communications", which can include voice and text communications. *TELUS*, however, was a case of statutory construction and not constitutional law.

Therefore, the stakes were high in *Marakah* and *Jones*. State access to text messaging raises unique concerns because it implicates not just privacy, but also expressive freedom. As Dickson C.J.C. wrote in *Canada (Human Rights Commission) v. Taylor*, "the freedoms of conscience, thought and belief are particularly engaged in a private setting."[15] Private communications are where we experiment with embryonic ideas, share our intimate thoughts, and express our rawest emotions. If the state is granted access to this category of information too easily, that "might well smother that spontaneity — reflected in frivolous, impetuous, sacrilegious, and defiant discourse — that liberates daily life."[16]

III. *MARAKAH* — TEXT MESSAGES ON THE RECIPIENT'S PHONE

The precise issue in *Marakah* was whether an individual can retain a reasonable expectation of privacy in his/her text messages once they are sent to and received on another person's device. This is a question of standing. Put another way, if A sends a text message to B, and the police discover that text message during a search of B's phone, does A have standing to challenge the constitutionality of the search? Writing on behalf of a five-judge majority, McLachlin C.J.C. said "yes". (Justice Moldaver dissented, with Côté J. joining him.)

---

[14] [2013] S.C.J. No. 16, 2013 SCC 16 (S.C.C.) [hereinafter "*TELUS*"].

[15] [1990] S.C.J. No. 129, [1990] 3 S.C.R. 892, at para. 77 (S.C.C.).

[16] *R. v. Duarte*, [1990] S.C.J. No. 2, [1990] 1 S.C.R. 30, at para. 42 (S.C.C.) [hereinafter "*Duarte*"], quoting from Harlan J. dissenting in *United States v. White*, 401 U.S. 745 (1971).

Chief Justice McLachlin reached this conclusion by applying the well-established "totality of the circumstances" test. The first factor of this test is the "subject matter of the search". This is where the Crown and defence typically fight over the framing of the issue.

One way to view the issue in *Marakah* is to view the subject matter of the search as being the recipient's phone. In this way, *Marakah* is all about the search of a device, and only the owner or user of that device has a reasonable expectation of privacy in its contents. Chief Justice McLachlin rejected that view.[17] Instead, she described the "subject matter of the search" as "... Mr. Marakah's 'electronic conversation' with Mr. Winchester".[18] She focused on text messages as a unique category of information, and focused on the substance of the information sought rather than the physical place in which it is found. She viewed this as a case of informational privacy rather than territorial privacy. Characterizing the subject matter of the search as an "electronic conversation" set the stage for the rest of McLachlin C.J.C.'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: *e.g.*, if the place is a dwelling, a high expectation of privacy is reasonable, but only for those who can control access to the dwelling like its residents.[19] Had McLachlin C.J.C. accepted that the subject of the search was the recipient's device (a physical location), the application of these factors would have been straightforward. But because she 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.

Chief Justice McLachlin's opinion is a textbook example of how to conduct a context-appropriate analysis. The "place of the search", she wrote, could be viewed as being the private electronic space that text

---

[17] *Marakah*, *supra*, note 2, at para. 16.

[18] *Id.*, at para. 17.

[19] Note that this principle may be revisited in *R. v. Le*, [2018] S.C.C.A. No. 34 (S.C.C.) (appeal from [2018] O.J. No. 359, 2018 ONCA 56 (Ont. C.A.)) [hereinafter "*Le*"].

messaging creates for the two parties to the conversation.[20] 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.[21] In the context of text messaging, individuals choose to disclose their private information to the recipient of the text message. That is a necessary part of engaging in the act of communication. While they lose "control" over the text message *vis-à-vis* the recipient, that should not result in them giving up their privacy rights in that communication *vis-à-vis* the rest of the world (and especially the state).[22] This analysis flowed directly from the way that McLachlin C.J.C. characterized the issue at the outset of her analysis.

Next, McLachlin C.J.C. set her sights on the most important factor in informational privacy cases: the nature of the information sought. The more private and revealing the information, the more likely it will attract constitutional protection. Here, McLachlin C.J.C. could have accepted an analogy that the Crown drew in its submissions: text messages are similar to letters. This analogy favoured the Crown because the sender of a letter does not retain any reasonable expectation of privacy in the letter once it is sent and received by the recipient. Only the recipient of the letter, in whose possession it lies, has standing to challenge an unconstitutional search and seizure of the letter.

Such backward-looking analogies, however, often fail to do justice to the true power of new technologies. Fortunately for the defence in *Marakah*, the Supreme Court had rejected similarly inapt comparisons in other cases. In *Vu*, the Court held that computers are not four-drawer filing cabinets.[23] In *Fearon*, the Court noted that cell phones are not briefcases.[24] And in *Marakah*, the Court effectively held (although it did not explicitly state) that text messages are not letters. Letters take days to be delivered to their recipient. One can meaningfully characterize a letter as having been "sent" once it is placed in the mail. Text messages, in

---

[20] *Marakah*, *supra*, note 2, at para. 28.

[21] *Id.*, at para. 39.

[22] *Id.*, at para. 40. To have held otherwise would have been to revive the long-discredited "risk analysis": the notion that we abandon all reasonable expectation of privacy whenever we run the risk that others might disseminate our private information. The Supreme Court has repeatedly (and wisely) rejected this doctrine: *Marakah*, *id.*, at para. 68; *Cole*, *supra*, note 10, at para. 76. This doctrine would be especially destructive of privacy in the digital world where there is always the risk that information will be leaked beyond our intended audience.

[23] *Vu*, *supra*, note 11, at para. 24.

[24] *Fearon*, *supra*, note 12, at para. 51.

contrast, are never simply "sent". Instead, they are part of an ongoing, dynamic dialogue that may continue indefinitely. Their instantaneous transmission allows for their conversational use.

Not only are text messages different from letters, but they are also different from non-written forms of communication in that they are *more* discreet. 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 C.J.C. put it colourfully:

> … 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.[25]

In light of all this, McLachlin C.J.C. 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. In most cases, the search will be unconstitutional unless police first obtain a warrant (or some other type of judicial authorization).[26]

This is as it should be. Text messaging may be, in many ways, the most discreet form of communication; but it is also the most recorded. By virtue of the technological medium used, text messaging creates at least two copies of each communication exchanged: one on the sender's phone and one on the recipient's phone.[27] As a result, nearly all of us are walking around with transcripts of years'-worth of private communications in our smartphones at all times. Even if we delete messages from our devices, they

---

[25] *Marakah*, *supra*, note 2, at para. 36.

[26] There are exceptions to the warrant requirement. If police conduct a lawful arrest, then they are entitled to conduct a limited search of the arrestee's smartphone upon arrest, including a review of recently sent or received text messages: *Fearon*, *supra*, note 12, at para. 76. Police can also conduct warrantless searches where there are exigent circumstances. In addition, individuals can waive their s. 8 rights by consenting to police searches.

[27] As illustrated in the companion appeal of *Jones*, *supra*, note 3, copies of text messages are also sometimes retained by the telecommunications service provider.

can be recovered forensically.[28] This makes it especially important for the law to step in and protect our text communications from disclosure to the state absent compliance with the Charter.

Marakah will have significant implications for how police conduct criminal investigations. The facts of *Marakah* concerned SMS text messages; but McLachlin C.J.C. made it clear that her reasoning would apply equally to other types of person-to-person communications tools, such as Apple iMessage, Google Hangouts, and Blackberry Messenger.[29] Indeed, one can easily extend this same reasoning to e-mails. While e-mails are sometimes used for lengthier and more formal communications than those found in text messages, that is not always the case. For many people, the decision of whether to send a message via SMS text messaging or e-mail turns on nothing more than which "app" they happen to click on first when they open their smartphone.

To be fair, McLachlin C.J.C. was careful to state that the exchange of electronic messages will not always attract a reasonable expectation of privacy.[30] But attention must be paid to the end of her opinion where she clarified this caveat with a few examples:

> … This is not to say, however, that every communication occurring through an electronic medium will attract a reasonable expectation of privacy and hence grant an accused standing to make arguments regarding s. 8 protection. This case does not concern, for example, messages posted on social media, conversations occurring in crowded Internet chat rooms, or comments posted on online message boards.[31]

A fair reading of these passages suggests that McLachlin C.J.C. intended to exclude from her opinion the types of communications that are exchanged in the electronic equivalent of the public square. One-to-one text messages, however, should generally attract a reasonable expectation of privacy in the post-*Marakah* world. The manner in which McLachlin C.J.C. applied the totality of the circumstances factors (*e.g.*, place of the search, control) would apply equally to all one-to-one communications.

Some of the post-*Marakah* commentary has focused on the fact that Mr. Marakah asked the recipient (Mr. Winchester) to delete the text message from his phone, and tried to argue that this distinguishes the text

---

28 *Vu*, *supra*, note 11, at para. 43.
29 *Marakah*, *supra*, note 2, at para. 18.
30 *Id.*, at para. 5.
31 *Id.*, at para. 55.

messages in this case as being more private than text messages in other cases. However, McLachlin C.J.C. relied on this fact solely to establish a *subjective* expectation of privacy, which is not a "high hurdle".[32] The bulk of the section 8 work is done when determining whether the accused has an *objectively* reasonable expectation of privacy. In this part of the analysis, the fact that Mr. Marakah asked Mr. Winchester to delete the messages played no role.

Finally, even in the case of group chats, a strong argument can be made that all participants in the chat enjoy a reasonable expectation of privacy. Many individuals use WhatsApp, for example, to participate in group chats with others in defined social circles (*e.g.*, high school friends). Just because more than one person is involved does not mean that the participants lose all expectation of privacy. *R. v. Wong* provides the best support for this proposition.[33] In that case, the appellant and 10 others were charged with keeping a common gaming house for operating a private gambling session in a hotel room. The police surreptitiously videotaped the operation. In the majority opinion, La Forest J. held that the accused had a reasonable expectation of privacy in the activities in the hotel room even though more than two people were involved and even though the public was invited to join the session. If this is true of the activities of a hotel room, then it should equally be true of the communications within a group chat.

IV. *JONES* — TEXT MESSAGES ON THE SERVER OF THE TELECOMMUNICATIONS PROVIDER

The companion case of *Jones* raised a more technical question: where the police are obtaining historical text messages from the servers of a third party service provider such as TELUS (as opposed to the recipient's phone), what type of court order do they need? An ordinary production order (for which the standard is the default test for reasonableness under section 8 of the Charter: reasonable and probable grounds) or the more rigorous Part VI authorization (otherwise known as a "wiretap" authorization, for which the police must also demonstrate "investigative necessity")?

In the 2013 case of *TELUS*, a plurality of the Supreme Court held that the police must obtain Part VI authorizations in order to acquire text

---

[32] *Id.*, at para. 23.

[33] [1990] S.C.J. No. 118, [1990] 3 S.C.R. 36 (S.C.C.).

messages from service providers on a prospective basis — that is, to obtain the production of *future* text messages. Should the standard be any different for *historical* text messages? Mr. Jones argued, "no".[34] Why should it matter whether the police seek judicial permission to acquire text messages the *day before* they come into existence, or the *day after*?

A majority of the Court disagreed with this argument. Writing on behalf of five justices, Côté J. explained that the distinction between historical and future communications is a meaningful one under Part VI of the *Criminal Code*. The threat posed by the latter is unique because "when equipped with sophisticated surveillance technologies, the state may be tempted to embark on forward-looking, 'fishing expedition[s] in the hope of uncovering evidence of crime'".[35] Therefore, a Part VI authorization is required for the latter but not the former.

Interestingly, Rowe J. wrote a separate concurring opinion in which he agreed with Côté J.'s interpretation of Part VI, but expressed concern that this enables the police to "*in effect* sidestep the requirements of Part VI by obtaining a production order immediately after the messages are sent."[36] He then explicitly stated that he was expressing "no settled view" on whether the ability of the police to obtain historical text messages with a production order (and not a Part VI authorization) is constitutional under section 8 of the Charter. It may not take long for enterprising defence counsel to see if they can get Rowe J. (or at least a judge of a lower court) to answer this question. *Jones* concerned the proper interpretation of Part VI of the *Criminal Code*, and not its constitutionality.

Jones also raised a second, more general issue concerning the litigation of section 8 Charter claims: in seeking to establish a *subjective* reasonable expectation of privacy (which is one of the requirements for standing under section 8), does the defence have to lead evidence? Or can the defence rely on the Crown's theory of the case? This has been a long-debated issue that often arises in drug possession cases. If the police find cocaine in a home, for instance, does A have to testify that he lives in the home in order to obtain standing to challenge the search of the home? Or can A simply rely on the Crown's theory that he lives there, which is why he is being prosecuted in the first place?

---

[34] The British Columbia Civil Liberties Association, for which the author was counsel, supported this position.

[35] *Jones*, *supra*, note 3, at para. 74.

[36] *Id.*, at para. 85 (emphasis in original).

Justice Côté's majority opinion endorsed the latter approach.[37] This is a significant decision for the criminal defence bar, who will no longer have to risk calling their client in a Charter *voir dire* to establish standing. While evidence in a *voir dire* is not automatically admissible in the trial proper, an admission at the *voir dire* can restrict the permissible scope of defence evidence and submissions at trial.[38] This is a gamble that defence counsel will no longer have to contemplate.

V. NEXT STEPS: *REEVES* AND *MILLS*

Marakah and *Jones* are two of the biggest section 8 Charter cases in a long time. Nonetheless, they do not answer all of the pressing digital privacy questions related to text communications. Less than one week after the Supreme Court released its judgments, the Court granted leave to appeal in two cases that will answer further questions about text message privacy and section 8 in general: *R. v. Reeves*[39] and *R. v. Mills*.[40]

1. *Reeves* — Who Can Consent?

Reeves will require the Court to confront the thorny issue of third party consent, last dealt with by the Supreme Court in *Cole*. Consenting to a police search is the equivalent of waiving one's right to be secure against unreasonable search and seizure. In order to be valid, it must be voluntary and informed. Thus, in *Cole*, the Court held that the School Board, which owned the laptop used by the accused school teacher, could not validly consent to a police search of the laptop's contents. Only the school teacher, as the user of the laptop and therefore the one with an expectation of privacy in its contents, could validly consent to a search. The School Board was a "third party". The Court emphatically rejected the American "third party consent" doctrine in Canada.[41]

In *Reeves*, the police seized a family computer that was co-owned by the accused and his spouse. The question was whether his spouse alone

---

[37] *Id.*, at para. 19.

[38] *Id.*, at para. 24.

[39] [2017] S.C.C.A. No. 275 (S.C.C.). The appeal was heard on May 17, 2018 and judgment was reserved.

[40] [2017] S.C.C.A. No. 125 (S.C.C.). The appeal was heard on May 25, 2018 and judgment was reserved. The author was counsel to the Criminal Lawyers' Association with Annamaria Enenajor.

[41] *Cole*, *supra*, note 10, at paras. 75-79.

could consent to the seizure. The Crown sought to distinguish *Cole* on the basis that the consenting party in that case (the School Board employer) did not have an "equal and overlapping privacy interest" in the subject of the search (the School Board-owned laptop) with the accused (a school teacher). The School Board's privacy interest was in the hardware (the physical device) rather than the software (the informational contents of the device). By contrast, so the argument went, the spouse's privacy interests and the accused's privacy interests in *Reeves* were coterminous.

The Ontario Court of Appeal held that the spouse's consent was valid, but purported to do so on a different basis from that advanced by the Crown. Rather than decide whether one party can waive the constitutional rights of another, the Court re-defined the scope of the accused's reasonable expectation of privacy and therefore his constitutional right. It would have been within the accused's "reasonable expectations" that his spouse might have "a legitimate interest in consenting to police access to the shared space and property."[42]

The Supreme Court heard the appeal in *Reeves* on May 17, 2018 and reserved judgment. How it decides the issue could have implications not just for police searches of shared computers, but also for searches of text messages. In *Marakah*, the Crown repeatedly raised this problem scenario: what happens when someone receives a threatening text message and wants to report it to the police? Can the recipient of that text consent to its seizure by the police? One way to answer this question would have been to adopt the line of reasoning advanced by the Crown in *Reeves.* Both the sender and recipient of the text message have equal and overlapping privacy interests in the electronic conversation; therefore, either party alone can validly consent. Neither the sender nor the recipient is a "third party", so the argument goes. Rather, they are both "first parties".[43]

This argument was made in *Marakah* but McLachlin C.J.C. did not accept it. Neither did she explicitly reject it. Rather, she merely observed that where an individual receives a threatening text message and alerts the police to its existence, the police can comply with section 8 by obtaining a warrant.[44] Of course, a warrant would only be necessary where there is no valid consent.

---

[42] *R. v. Reeves*, [2017] O.J. No. 3038, 2017 ONCA 365, at para. 62 (S.C.C.).

[43] Indeed, the Criminal Lawyers' Association advanced this position at the Supreme Court in *Marakah*, *supra*, note 2.

[44] *Id.*, at para. 50. This argument was made by the British Columbia Civil Liberties Association, for which the author was counsel.

Whether *Marakah* will be interpreted as having rejected the notion that the recipient of a text message can unilaterally consent to its seizure by the police may be clarified when the Court decides *Reeves*. Should the Court conduct a full-scale analysis of the law of consent, one hopes that it will keep the following stages of the section 8 analysis distinct:

1. *Is there state action*? The Charter applies to state action. Where the state actor is merely a passive recipient of information, such as in the case of a victim who reports a threatening text message to the police, it is questionable whether the Charter applies.[45] The situation would be different, however, where the victim chooses not to report the threat but the police discover it through some other means, and then attempt to seize the text message from the victim. In the latter scenario, the state is not merely a passive recipient of information but is actively seeking it out. Therefore, the Charter should apply.

2. *Does the state action invade a reasonable expectation of privacy*? If there is state action, the next question is whether that state action invades a reasonable expectation of privacy such that there is a search or seizure within the meaning of section 8 of the Charter. The test for answering this question is the totality of the circumstances test established in *R. v. Edwards*[46] and adapted to the informational privacy context in *Spencer*.[47]

3. *Who can consent to the privacy invasion*? It is only after the first two questions are answered that the Court should move onto this third question. If there is state action so as to engage the Charter, and that state action invades a reasonable expectation of privacy, then section 8 of the Charter is engaged — and the individual whose privacy is invaded has the right to waive his or her section 8 rights by consenting to a police search. It is difficult to see how another party, however, can waive these rights on that individual's behalf — even if the two parties have "equal and overlapping" privacy interests.

---

[45] See Doherty J.A.'s analysis in *R. v. Orlandis-Habsburgo*, [2017] O.J. No. 4143, 2017 ONCA 649, at para. 34 (Ont. C.A.).

[46] [1996] S.C.J. No. 11, [1996] 1 S.C.R. 128 (S.C.C.). Note that this test may be revisited in *Le*, *supra*, note 19.

[47] *Spencer*, *supra*, note 13, at paras. 17-21.

2. *Mills* — What About Undercover Officers?

A different but related issue is raised by *Mills*. What if the recipient of a text message is an undercover police officer? Can that police officer capture the text message as he is receiving it and, by doing so, seize the communication for investigative purposes? If this were a phone call, the undercover police officer would have to obtain prior judicial authorization before recording the call. The Supreme Court decided that in *Duarte* nearly 30 years ago.[48] Should the law be any different for a text communication?

The Newfoundland and Labrador Court of Appeal answered "yes". It held that individuals have no reasonable expectation of privacy in messages sent to an undercover officer. But it did so on the basis that "as the sender of such communications, Mr. Mills must have known that he lost control over any expectation of confidentiality" and "took a risk when he voluntarily communicated with someone he did not know".[49] This sort of risk analysis is similar to the line of reasoning that McLachlin C.J.C. rejected in *Marakah*.[50] Other lower court cases have reached the same conclusion applying the same, now-discredited reasoning.[51] These cases should have little currency in the post-*Marakah* world.

The only fact that separates the text communications in *Mills* from those in *Marakah* is the fact that Mr. Mills had never physically met the undercover officer with whom he was communicating. In that sense, the recipient of the text messages was a "stranger". This should not, however, negate a reasonable expectation of privacy. One can imagine any number of intensely private electronic conversations that individuals have with those whom they have never met in person. This happens every day with online dating. It happens when Canadians seek medical advice from an online doctor.[52] It happens every time a prospective client sends an e-mail to a lawyer seeking legal assistance. It would be strange if these electronic communications did not attract a reasonable expectation of privacy simply because the parties had never met in person.[53]

---

[48] *Supra*, note 16.

[49] *R. v. Mills*, [2017] N.J. No. 55, 2017 NLCA 12, at para. 23 (N.L.C.A.).

[50] *Marakah*, *supra*, note 2, at paras. 45, 68.

[51] *R. v. Allen,* [2017] O.J. No. 4239, 2017 ONSC 1712, at para. 46 (Ont. S.C.J.); *R. v. Ghotra*, [2015] O.J. No. 7253, at para. 125 (Ont. S.C.J.); *R. v. Merritt*, [2017] O.J. No. 6928, 2017 ONSC 1648, at para. 46 (Ont. S.C.J.). See *contra*, *R. v. Kwok*, [2008] O.J. No. 2414, at paras. 19, 22 (Ont. C.J.).

[52] CBC News, "Online doctor consultations take off in Canada" (July 12, 2017), online: <https://www.cbc.ca/news/health/virtual-medical-consults-1.4200397>.

[53] See Steven Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap" (May 8, 2018), online: SSRN <https://ssrn.com/abstract=>, at 25-26 [hereinafter "Penney"].

TELUS provides another important reference point for the issue in *Mills*. In *TELUS*, the plurality held that police have to obtain judicial authorization (under Part VI) to acquire copies of text messages from a telecommunications provider on a prospective basis. The only difference between that technique and what the police did in *Mills* is that, in the case of the latter, the police cut out the middleman. Rather than going through a telecommunications provider, the police acquired copies of text messages by virtue of being a party to the conversation itself. In both cases, the police engaged in communications surveillance. The distinction is simply that of third party surveillance (*TELUS*) versus participant surveillance (*Mills*). *Duarte* tells us that is a distinction without a difference when it comes to the applicability of section 8 of the Charter.[54]

If the Supreme Court overturns the Court of Appeal's reasoning in *Mills*, as it should, police will generally need to obtain judicial authorization before exchanging and recording text messages with an investigative target. The applicable provision would be section 184.2(1) in Part VI of the *Criminal Code*. This provision was enacted after the Court decided *Duarte* in 1990. It applies when the police seek to "intercept" a "private communication" — even when the officer doing the intercepting is a participant to the communication.

Section 183 of the *Criminal Code* defines "intercept" broadly to include the acts of "listen[ing] to, record[ing] or acquir[ing] a communication or acquir[ing] the substance, meaning or purport thereof". It would therefore capture the act of an undercover officer participating in and recording a text communication with the investigative target. And in *TELUS*, the Supreme Court unanimously held that text messages are "private communications".[55]

To apply Part VI in this manner should not unduly hamper the ability of the police to combat crimes such as child luring. It's true that police would not be able to use private text communications to develop reasonable and probable grounds; they would need those grounds at the outset before they engage in any private text communications. But this would not prevent the police from developing the requisite grounds in a public chatroom. Electronic communications in public chatrooms are

---

[54] *Duarte*, *supra*, note 16, at para. 28. Parliament has since recognized that we have a stronger expectation of privacy against third party surveillance. Thus, investigative necessity is an added requirement for third party interceptions under the *Criminal Code*, s. 186, but is not a requirement for one-party consent authorizations under s. 184.2. See Penney, *id.*, at 35.

[55] *Supra*, note 14, at para. 12, *per* Abella J., at para. 67, *per* Moldaver J., and at para. 135, *per* Cromwell J.

arguably not private communications under Part VI, nor would they attract the protections of section 8 of the Charter. Indeed, McLachlin C.J.C. referred specifically to messages exchanged in "crowded Internet chat rooms" as one type of electronic communication that may fall outside the scope of *Marakah*. Therefore, police would be free to exchange messages in this environment without any grounds. They would only need the grounds to obtain judicial authorization (under *Criminal Code*, section 184.2) when they choose to move the communication from a public chatroom into a private, one-to-one context. Many child luring investigations proceed in exactly this manner.[56]

VI. BEYOND THE CRIMINAL LAW

Marakah's ramifications will not be limited to the criminal law. Its impacts will likely be felt in at least two other areas: regulatory investigations and the development of the tort of intrusion upon seclusion.

Regulatory investigations will be affected because the Charter applies to all government entities, including both police conducting criminal investigations and regulatory bodies conducting regulatory investigations.

Of course, the way in which the Charter applies may differ in the regulatory context as compared to the criminal context. In a number of cases in the early- to mid-90s, the Supreme Court of Canada relaxed the ordinary *Hunter v. Southam* standards for a reasonable search and seizure under section 8 ("prior judicial authorization" and "reasonable and probable grounds") in the regulatory context.[57] In each of these cases, however, context was a proxy for privacy. Inspections of business records did not have to meet the ordinary standards of section 8 because they engaged a lower expectation of privacy.[58] But as Wilson J. wrote in

---

[56] *R. v. Legare*, [2009] S.C.J. No. 56, [2009] 3 S.C.R. 551, at para. 8 (S.C.C.); *R. v. Thain*, [2009] O.J. No. 1022, 2009 ONCA 223, at para. 2 (Ont. C.A.); *R. v. Pengelley*, [2010] O.J. No. 4174, 2010 ONSC 5488, at para. 2 (Ont. S.C.J.); *R. v. Ghotra*, [2016] O.J. No. 1688, 2016 ONSC 5675, at para. 51 (Ont. S.C.J.).

[57] [1984] S.C.J. No. 36, [1984] 2 S.C.R. 145 (S.C.C.).

[58] See, for example, *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] S.C.J. No. 23, [1990] 1 S.C.R. 425 (S.C.C.); *British Columbia (Securities Commission) v. Branch*, [1995] S.C.J. No. 32, [1995] 2 S.C.R. 3 (S.C.C.). See also *Cole*, *supra*, note 10, at paras. 70-71, wherein Fish J. referred to a number of cases in the early 2000s, including *R. v. Jarvis*, [2002] S.C.J. No. 76, 2002 SCC 73 (S.C.C.), and characterized them as follows: "... In each instance, given the regulated nature of the documents in question, the individual claiming the protection of s. 8 did not have a reasonable expectation of preventing or controlling the further dissemination of his or her information to the law

R. v. McKinlay Transport, "[t]he greater the intrusion into the privacy interests of an individual, the more likely it will be that safeguards akin to those in *Hunter* will be required."[59] Therefore, in the subsequent case of *Baron v. Canada*, the Court held that where the state seeks to do something as intrusive as searching a private residence, the state must obtain prior judicial authorization even though the search is conducted for a regulatory (and not criminal) purpose.[60]

Following this reasoning, where a regulatory body seeks access to private text communications, which can reveal our most intimate thoughts and feelings, it may be argued that section 8 of the Charter should apply with close to full force. In most cases, this will require the regulatory body to obtain prior judicial authorization on the basis of "reasonable grounds" before searching or seizing the text communications regardless of whose device is targeted.

Marakah may also affect the development of the tort of intrusion upon seclusion. The tort is made out where (i) the defendant's conduct is intentional (or reckless); (ii) the defendant invades, "without lawful justification", the plaintiff's private areas or concerns; and (iii) "a reasonable person would regard the invasion as highly offensive causing distress, humiliation, or anguish."[61]

In establishing this tort, the Ontario Court of Appeal cited the right to privacy in section 8 of the Charter and the need for the common law to evolve in accordance with Charter values.[62] It follows that the courts should also *develop* the tort in accordance with section 8 case law — including, most recently, *Marakah*. Accordingly, where a business

---

enforcement branch of the state." Each of these cases involved documents created and maintained in a highly regulatory environment. They did not involve something as inherently private as private communications.

[59] [1990] S.C.J. No. 25, [1990] 1 S.C.R. 627, at 649 (S.C.C.).

[60] [1993] S.C.J. No. 6, [1993] 1 S.C.R. 416, at paras. 37-40 (S.C.C.). See, however, *Law Society of Alberta v. Sidhu*, [2017] A.J. No. 691, 2017 ABCA 224 (Alta. C.A.). In *Sidhu*, the Law Society investigator requested that the Appellant produce access to records related to his desktop computers, laptops, iPads, tablets, cellular telephones, *etc.* The Alberta Court of Appeal held that the Appellant had a lower expectation of privacy in the contents of his devices because he was a regulated legal professional — even though searches of digital devices are ordinarily considered highly invasive. The Court wrote that (at para. 20) "[w]ith the regulatory context comes an attenuated expectation of privacy because there is an awareness and acceptance that the regulator will be involved in the life and practice of that field". This applies to information stored on digital devices even though such information may engage details related to the regulated individual's personal life because "[t]he power of investigation in professional misconduct extends to a professional's personal life that reflects on their integrity" (at para. 23).

[61] *Jones v. Tsige*, [2012] O.J. No. 148, 2012 ONCA 32, at para. 71 (Ont. C.A.).

[62] *Id.*, at para. 46.

intentionally or recklessly accesses private text communications (including e-mail) without lawful justification, it may find itself on the receiving end of an intrusion upon seclusion claim. And where that claim is in the form of a class proceeding,[63] the class may include not just the employees or accountholders whose text communications were accessed, but all those with whom they were communicating. This could significantly enlarge the class and therefore the liability that a defendant may face.

Even where a business does not intentionally or recklessly access private text communications, but merely stores them in a manner making them vulnerable to hackers, that may be the subject of an intrusion upon seclusion claim. In the recent case of *Agnew-Americano v. Equifax Canada Inc.*, the Court held that it was neither "frivolous" nor "fanciful" to base an intrusion upon seclusion claim on the mere creation of risk of allowing hackers access to unauthorized information.[64]

VII. CONCLUSION

Texting is paradoxically the most discreet and most recorded form of communication. Like many activities we now engage in with our smartphones, we are addicted to the convenience, recognize the risks of our information leaking out to the public, and expect everyone to act responsibly to prevent those leaks — all at the same time. The law should develop in accordance with these evolving social norms. While one can criticize the Court for not going far enough in *Jones*, we are fortunate to have a Supreme Court that has (for the most part) led with wisdom in this area. As Côté J. put it in the companion case of *Jones*, "... Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives."[65] One hopes that the Court will continue this trend in the upcoming cases of *Reeves* and *Mills.*

---

[63] See, *e.g.*, *Bennett v. Lenovo (Canada) Inc.*, [2017] O.J. No. 784, 2017 ONSC 1082, at paras. 17-23 (Ont. S.C.J.).

[64] [2018] O.J. No. 361, 2018 ONSC 275, at paras. 138-163 (Ont. S.C.J.). The precedential value of this decision may be limited because it was merely a "carriage" ruling in a class proceeding.

[65] *Jones*, *supra*, note 3, at para. 45.