CONSENT SEARCHES FOR ELECTRONIC TEXT COMMUNICATIONS: ESCAPING THE ZERO-SUM TRAP

STEVEN PENNEY*

In R. v. Marakah, *a majority of the Supreme Court of Canada decided that senders of electronic text communications maintain a reasonable expectation of privacy over their messages even after they are copied to recipients' devices. The dissenters argued, in contrast, that any such expectation is objectively unreasonable given senders' inability to control the messages after delivery. The Supreme Court did not settle the question, however, of whether this expectation can be defeated by a recipient's voluntary decision to allow police to search his or her own device. Indeed, each side intimated that such a consent would be difficult, if not impossible, to obtain.*

This article argues, nonetheless, that courts can and should use consent doctrine to avoid the "zero-sum" model of section 8 adjudication that characterizes the majority and dissenting reasons in Marakah. *Properly interpreted, that doctrine preserves* Marakah*'s core holding — that senders do not reasonably expect unfettered state access to their received text communications — while also giving effect to recipients' autonomous decisions to assist police.*

However, as with oral communications, a recipient's consent to disclose a sender's text communications to police should only defeat the sender's expectation of privacy over preexisting messages. Contrary to several lower court decisions, this article argues that the acquisition of future, incoming communications from recipients' devices (with or without consent) invades senders' reasonable expectations of privacy under section 8 of the Charter *and constitutes an "interception" requiring judicial authorization under section 184.2 of the* Criminal Code.

TABLE OF CONTENTS

I. INTRODUCTION 2
II. *MARAKAH* AND THE ZERO-SUM GAME 5
III. CONSENT SEARCH JURISPRUDENCE 7
A. FIRST-PARTY CONSENT 7
B. THIRD-PARTY CONSENT 9
IV. APPLYING CONSENT DOCTRINE TO TEXT SEARCHES 11
A. AUTHORITY TO CONSENT 12
B. VOLUNTARY AND INFORMED 15
V. PROSPECTIVE SURVEILLANCE FROM RECIPIENTS' DEVICES 16
A. CONSENT 17
B. PRIVATE COMMUNICATION 18
C. INTERCEPT 20
VI. CONCLUSION 26

* Professor, Faculty of Law, University of Alberta.

I. INTRODUCTION

Most conversations in the pre-digital era were oral, and therefore largely ephemeral. Whether face-to-face or by telephone, oral conversations were rarely recorded and stored. Text communications (such as letters) existed, of course, but were less common and less conversational.[1] The vast proportion of interpersonal communication was therefore unavailable for verifiable retrieval. This mitigated the risks of revealing confidences to others: absent surreptitious recording, speakers could contest listeners' accounts of conversation.

The digital communications revolution has upended this calculus. As conversations are increasingly encoded in digital form, they are more likely to be recorded and stored and therefore accessible to third parties, including law enforcement.[2] This poses a substantial threat to communications privacy and the social interests it serves. If recorded conversations are not reasonably secure from unauthorized use, people will be less likely to communicate in efficient, candid, and socially productive ways.[3]

Courts and legislatures have responded to this threat by protecting the privacy of digital text communications in a variety of circumstances.[4] The decisions to do so were often uncontroversial. Few would argue, for example, that police should have free reign to obtain text communications from suspects' own devices.[5] There is also a consensus (in Canada at least) that digital communications remain protected even when obtained from third-party service providers.[6]

It is sometimes more difficult, however, to decide whether to protect the privacy of text communications. In *R. v. Marakah*, the courts divided over whether police violated the accused's section 8 *Charter*[7] right to be free from unreasonable search or seizure when they illegally seized his accomplice's phone and retrieved text messages sent by the accused. The applications judge[8] and majority of the Court of Appeal[9] concluded that there was no

---

1 See *R v Marakah*, 2017 SCC 59 [*Marakah* SCC] ("[t]he quantity of information they contain and the speed at which they are transmitted give text messages a conversational quality that differs markedly from letters" at para 87, Rowe J, concurring).

2 See generally *R v Pelucco*, 2015 BCCA 370 at paras 64–65 [*Pelucco*]; *R v SM*, 2012 ONSC 2949 at para 18.

3 See Richard A Posner, "The 1978 James McCormick Mitchell Lecture: Privacy, Secrecy, and Reputation" (1979) 28:1 Buff L Rev 1 at 17; Charles J Hartmann & Stephen M Renas, "Anglo-American Privacy Law: An Economic Analysis" (1985) 5:2 Intl Rev L & Econ 133 at 145; Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97:2 J Crim L & Criminology 477 at 492–93; Anthony G Amsterdam, "Perspectives on the Fourth Amendment" (1974) 58:3 Minn L Rev 349 at 388.

4 See generally Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12:2 Can Crim L Rev 115 at 125–29.

5 See *R v Fearon*, 2014 SCC 77 at paras 51–58 [*Fearon*] (implicitly recognizing a reasonable expectation of privacy in text communications found on an accused's phone seized incident to arrest); *R v Weir*, 1998 ABQB 56, aff'd 2001 ABCA 181 (recognizing reasonable expectation of privacy in email).

6 See *R v TELUS Communications Co*, 2013 SCC 16 [*Telus*] (recognizing a reasonable expectation of privacy in text messages and prohibiting prospective acquisition from service providers outside of Part VI of the *Criminal Code*); *R v Jones*, 2017 SCC 60 at paras 38–55 [*Jones*] (recognizing a sender's reasonable expectation of privacy in text messages stored by service provider).

7 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

8 *R v Marakah*, 2014 ONSC 7580, aff'd 2016 ONCA 542 [*Marakah* CA], rev'd *Marakah* SCC, *supra* note 1.

9 *Marakah* CA, *ibid*.

violation, holding that senders lack a reasonable expectation of privacy over messages acquired from recipients' devices.[10]

The Supreme Court reversed (5:2), with the majority deciding that senders generally maintain a reasonable expectation of privacy over text messages[11] even after they are copied to recipients' devices.[12] The dissenters argued, in contrast, that any expectation of privacy that senders may have is objectively unreasonable given their utter inability to control the messages after delivery.[13]

Marakah thus settles the question of whether senders maintain an expectation of privacy in messages stored on recipients' devices. If police gain access to someone's device, people who have sent that person text communications will have standing to claim that police violated their section 8 rights. As occurred in *Marakah*, that claim will likely be successful if police discovered the sender's messages after illegally seizing or searching the recipient's device.[14]

The Supreme Court in *Marakah* did not discuss, however, whether section 8 protects received messages on a device that police have lawfully obtained. Police may lawfully access devices in two relevant ways: with the user's consent and without it. If police seize a device without consent, they may search it for evidence (including text communications) under the aegis of any law that authorized the seizure and search, such as the common law power to search incident to arrest[15] or a statutory power to search under warrant.[16] In exercising these powers, police may retrieve received messages, including any found in "plain view."[17] If police adhere to the search power's parameters, they will not violate senders' section 8 rights.[18]

---

10 This is because there is no "search or seizure," and thus no potential section 8 infringement, unless a state actor invades the accused's own reasonable expectation of privacy. See *R v Edwards*, [1996] 1 SCR 128 at paras 34–43; *R v Wise*, [1992] 1 SCR 527 at 533.

11 I do not distinguish between different types of private, electronic text communications. Though *Marakah* dealt only with "short message service" (sms) communications, I assume that email and other internet-enabled communications services should be treated in the same manner. See *R v Pammett*, 2014 ONSC 1213 ("I utterly fail to see the distinction between a text message and an email for the purposes of determining whether there is a reasonable expectation of privacy" at para 9).

12 *Marakah* SCC, *supra* note 1. The majority reasons were penned by Chief Justice McLachlin and joined by Justices Abella, Karakatsanis, and Gascon. Justice Rowe wrote separately, concurring with the majority's disposition of the case as well as its "general approach … with respect to the existence of a reasonable expectation of privacy" (*ibid* at para 88, Rowe J, concurring).

13 *Ibid* at paras 112–48, Moldaver J, dissenting. Justice Moldaver wrote for himself and Justice Côté.

14 See *ibid* at paras 56–57.

15 See *Fearon*, *supra* note 5 (police may conduct a limited search of the arrestee's device in certain circumstances as an incident of arrest).

16 See e.g. *Criminal Code*, RSC 1985, c C-46 (power to search for computer data included within general power to search "building, receptacle or place," ss 487(2.1)–(2.2)); *R v Vu*, 2013 SCC 60 [*Vu*] (digital data cannot be searched under warrant without specific authorization).

17 The plain view doctrine exists both at common law and under section 489(1) of the *Criminal Code*, *ibid* and section 11(8) of the *Controlled Drugs and Substances Act*, SC 1996, c 19. Briefly stated, the doctrine permits police to seize items of obvious evidentiary significance when they are engaged in lawful activities in a domain that they are lawfully permitted access to. See *R v Jones*, 2011 ONCA 632 at paras 53–64 (applying plain view doctrine to computer searches). See also generally Steven Penney, Vincenzo Rondinelli & James Stribopoulos, *Criminal Procedure in Canada*, 2nd ed (Markham: LexisNexis, 2018), §§3.265–3.273.

18 See Simon Stern, "Textual Privacy and Mobile Information" (2018) 13:17 Osgoode Hall Law School Legal Studies Research Paper Series, Research Paper No 79 at 1, 44–45, online: Social Science Research Network <https://ssrn.com/abstract=3165029>.

It is not as clear, however, whether police may obtain received messages on the recipient's consent. The majority and dissenting justices in *Marakah* alluded to the question, but neither resolved it.[19] This is unfortunate. Consent doctrine has the potential to bridge the gap between the two sides and achieve a better accommodation between communications privacy and crime control.

I argue, nonetheless, that courts can and should use consent doctrine to avoid the "zero-sum" model of section 8 adjudication that characterizes the majority and dissenting reasons in *Marakah*. Properly interpreted, that doctrine preserves *Marakah*'s core holding — that senders do not reasonably expect unfettered state access to their received text communications — while also giving effect to recipients' autonomous decisions to assist police.

However, as with oral communications, a recipient's consent to disclose a sender's text communications to police should only defeat the sender's expectation of privacy over preexisting messages. Contrary to several lower court decisions, I argue that the acquisition of future, incoming communications from recipients' devices (with or without consent) invades senders' reasonable expectations of privacy under section 8 of the *Charter* and constitutes an "interception" requiring judicial authorization under section 184.2 of the *Criminal Code*.[20]

The remainder of the article proceeds as follows. Part II undertakes a close reading of the majority and dissenting reasons in *Marakah*, highlighting their zero-sum orientation. In Part III, I examine the consent search jurisprudence, outlining the requirements for "first-party" and "third-party" consent. The former involves the familiar inquiry into whether a person's purported agreement to assist police was sufficiently voluntary and informed to defeat his or her own entitlement to legal protection. The latter arises when one person has the lawful authority to consent to a search of a domain over which another person also has a reasonable expectation of privacy. Part IV applies these doctrines to retrospective searches for received text communications on digital devices, arguing that parties to text conversations have a shared expectation of privacy over the conversation that can be defeated by one party's voluntary and informed consent. In Part V, I examine the prospective acquisition of text communications from recipients' devices, arguing that the *Charter* and *Criminal Code* compel police to obtain "participant" interception authorizations under Part VI of the *Criminal Code* to conduct this kind of surveillance. Part VI concludes.

---

19 *Marakah* SCC, *supra* note 1 at paras 49–51, 182–84, Moldaver J, dissenting.

20 This issue will likely be addressed in the Supreme Court of Canada's upcoming decision in *R v Mills*, 2017 NLCA 12 [*Mills* CA], leave to appeal to SCC granted, 37518 (14 December 2017), which was heard and reserved on 25 May 2018. See discussion in Part V.B, below.

II. *MARAKAH* AND THE ZERO-SUM GAME

The majority and dissenting reasons in *Marakah* hew closely to what Ric Simmons has called the zero-sum model of search and seizure adjudication.[21] In this model, cases (especially the type of marginal, "close" cases most likely to be decided by high courts) are conceived as battles between incommensurate values or preferences: individual privacy and liberty versus security and crime control. Courts obviously attempt to achieve a reasonable balance between these interests. And they may also try to craft rules minimizing adverse effects for the losing side. But in the end, the court favours one interest over the other. Dissenting judges and critics are left to poke holes in the court's reasoning and assert the superiority of the contrary position. And while observers will contend that one side or the other had the better doctrinal, theoretical, or empirical case, most will conclude that the outcome was driven chiefly by the judges' *ex ante* normative preferences.[22]

The justices who wrote in *Marakah* did share certain assumptions. Unsurprisingly, they agreed on the (highly flexible[23]) analytical framework for deciding whether police invaded the applicant's reasonable expectation of privacy under section 8.[24] This requires an assessment of the "totality of the circumstances" involving four lines of inquiry: (1) defining the subject matter of the search, (2) determining whether the claimant had a direct interest in that subject matter, (3) determining whether the claimant had a subjective expectation of privacy in the subject matter, and (4) deciding whether any subjective expectation of privacy was objectively reasonable.[25] The claim will not succeed unless the answer to each of questions (2)-(4) is "yes." If so, the court will go on to consider whether the intrusion onto the reasonable expectation of privacy (that is, the "search or seizure") was reasonable under section 8.[26] The justices also agreed that the "subject matter" of the search was the "electronic conversation" between the accused and his accomplice.[27] Nor was there any dispute over whether the accused had a direct interest and subjective expectation of privacy in that conversation: each side answered "yes" to both questions.[28]

As usual, the debate centred around whether that expectation was objectively reasonable. In her reasons, Chief Justice McLachlin focused on digital text communication as a social practice, stressing that it often reveals inherently private aspects of the individual's "biographical core."[29] "Electronic conversations," she wrote, "can allow people to

---

21 Ric Simmons, "Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment" (2013) 36:2 Harv J L & Pub Pol'y 549. On people's tendency to characterize transactions as zero-sum when they are not, see Thomas Sowell, *Economic Facts and Fallacies* (New York: Basic Books, 2008) at 3–6; Samuel GB Johnson, Jiewen Zhang & Frank C Keil, "Psychological Underpinnings of Zero-Sum Thinking" (28 January 2018), online: Social Science Research Network <https://ssrn.com/abstract=3117627>.

22 See generally Jeffrey A Segal, Harold J Spaeth & Sara C Benesh, *The Supreme Court in the American Legal System* (Cambridge: Cambridge University Press, 2005); Frank B Cross, *Decision Making in the U.S. Courts of Appeals* (Stanford: Stanford University Press, 2007).

23 See *R v Tessling*, 2004 SCC 67 at para 31 [*Tessling*]; *R v Spencer*, 2014 SCC 43 at para 17 [*Spencer*]; *Marakah* SCC, *supra* note 1 at paras 115–17, Moldaver J, dissenting.

24 *Marakah* SCC, *ibid* at paras 10–12, McLachlin CJC, para 84, Rowe J, paras 105–108, Moldaver J.

25 See *R v Cole*, 2012 SCC 53 at para 40 [*Cole*]; *Spencer*, *supra* note 23 at para 18; *R v Patrick*, 2009 SCC 17 at para 27 [*Patrick*]; *Tessling*, *supra* note 23 at para 32.

26 See *Marakah* SCC, *supra* note 1 at paras 7, 56.

27 *Ibid* at para 17, McLachlin CJC, para 87, Rowe J, paras 94, 111, Moldaver J. See also *Jones*, *supra* note 6 at para 14; *Telus*, *supra* note 6 at para 5, Abella J.

28 *Marakah* SCC, *ibid* at paras 21–23, McLachlin CJC, para 102, Moldaver J.

29 *Ibid* at paras 31–37.

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."[30] The fact that the sender of a message loses control over it after it reaches the recipient, she insisted, does not extinguish that expectation. Evoking Justice La Forest in *R. v. Duarte*, she noted that while people inevitably court betrayal when they share confidences, this risk is "of a different order" than that of unfettered state access to stored communications.[31]

In his dissenting reasons, Justice Moldaver agreed that text messages are inherently private and that section 8 is engaged when they are obtained from senders' devices or service providers.[32] But as senders cannot prevent further dissemination after their messages are received, section 8 does not apply when police obtain them from recipient's devices.[33] "[A] person's expectation of privacy in informational subject matter that falls under another person's exclusive control," he wrote, "cannot be reasonable in a society that values the freedom of individuals to share information."[34]

The majority and dissenting justices also disagreed about the practical consequences of protecting received messages under section 8. Justice Moldaver warned that it would unjustifiably limit law enforcement's ability to obtain threatening, violent, or abusive communications from victims' devices.[35] He also predicted that it would complicate attempts to obtain evidence from recipients' devices on consent, generate needlessly complex litigation, and cause police to waste resources obtaining search warrants for basic investigative information.[36] "[E]xpanding the scope of persons who can bring a s. 8 challenge," he asserted, "risks disrupting the delicate balance that s. 8 strives to achieve between privacy and law enforcement interests, particularly in respect of offences that target the most vulnerable members of our society, including children, the elderly, and people with mental disabilities."[37]

Chief Justice McLachlin, in contrast, discounted the detrimental impact of the Supreme Court's holding on law enforcement. If recipients of incriminating text communications tell police about them, she reasoned, police will normally be able to get a warrant to seize and search their devices.[38] And if police obtain such messages without a warrant, the prosecution may still argue that the search was reasonable under section 8 or that the messages should be admitted despite the *Charter* breach under section 24(2).[39] In any case, she concluded,

---

30 *Ibid* at para 36. Chief Justice McLachlin also explained that the "zone of privacy" that people reasonably expect regarding their electronic conversations "extends beyond one's own mobile device; it can include the electronic conversations in which one shares private information with others" (*ibid* at para 37).

31 *Ibid* at paras 40–45, citing *R v Duarte*, [1990] 1 SCR 30 at 44 [*Duarte*].

32 *Ibid* at paras 92, 106, 127, 140, 146–47.

33 *Ibid* at paras 98–99, 113–48, 173, 177.

34 *Ibid* at para 129.

35 *Ibid* at paras 168–69, 175.

36 *Ibid* at paras 181–88.

37 *Ibid* at para 100. Justice Moldaver also concluded that "the cumulative effect of the practical concerns for law enforcement and the administration of criminal justice weighs heavily in favour of denying standing to claimants such as Mr. Marakah" (*ibid* at para 188).

38 *Ibid* at para 50.

39 *Ibid* at paras 51–52.

"[w]hatever law enforcement's interest in enjoying unfettered access to individuals' text messages, privacy in electronic conversations is worthy of constitutional protection."[40]

It is inevitable that judges will have divergent preferences, that these preferences will shape their decisions, and that these decisions will often benefit one legitimate social interest at another's expense.[41] There are undoubtedly section 8 cases where law enforcement must inevitably take a back seat to privacy (and vice versa). But countervailing interests are not always as incommensurable as they seem, and it is possible in some search and seizure cases to (largely) escape the zero-sum calculus. In the remainder of this article I explain how the Supreme Court's jurisprudence on digital privacy can be interpreted to maximize both digital communications privacy *and* law enforcement efficacy in the context of searches for received electronic text communications.

III. CONSENT SEARCH JURISPRUDENCE

The key to unlocking *Marakah*'s positive-sum potential is the concept of the "consent search," of which there are two types: first-party and third-party. In first-party consent claims, the prosecutor asserts that the accused waived his or her entitlement to section 8 protection.[42] For third-party consent, the prosecutor alleges that someone other than the accused lawfully acceded to a search of a domain over which both the accused and third party had a reasonable expectation of privacy. I deal with each in turn below.

A. FIRST-PARTY CONSENT

Like any other *Charter* right, people may waive their right to be free from unreasonable search or seizure.[43] As explained in *R. v. Wills*,[44] when "one consents to the police taking something that they otherwise have no right to take, one relinquishes one's right to be left alone by the state."[45] Consent is only relevant, of course, if the subject has a reasonable expectation of privacy in the circumstances. If not, as discussed above, there is no "search or seizure" and therefore no section 8 violation, regardless of consent. But if a person with a reasonable expectation of privacy lawfully consents, and police adhere to the scope of that

---

40 *Ibid* at para 53. See also *ibid*, citing *R v Plant*, [1993] 3 SCR 281 at 293: unfettered state access to electronic conversation "is outweighed by 'the societal interests in protecting individual dignity, integrity and autonomy.'" Though he agreed with the majority's conclusion and "general approach" to the reasonable expectation of privacy analysis, Justice Rowe nonetheless expressed reservations about its practical implications in a similar manner to Justice Moldaver. He concluded, however, that these concerns did not arise on the facts and that "principle and practicality must not be strangers in the application of s. 8 or we might well thwart justice in the course of seeking to achieve it" (*ibid* at paras 88–89, Rowe J, concurring).

41 See generally Lee Epstein, William M Landes & Richard A Posner, *The Behavior of Federal Judges: A Theoretical and Empirical Study of Rational Choice* (Cambridge, Mass: Harvard University Press, 2013).

42 As consent searches are warrantless, the prosecution bears the burden of establishing their lawfulness. See *Hunter v Southam Inc*, [1984] 2 SCR 145 at 161; *R v Wills* (1992), 7 OR (3d) 337 (CA) [*Wills*]. See also *Young v Ewatski*, 2012 MBCA 64 at paras 49–58, leave to appeal to SCC refused, 35035 (28 March 2013) (burden to prove consent to search falls on the Crown as the defendant in a civil action); *Everett v McCaskill*, 2015 MBCA 107 at para 16, leave to appeal to SCC refused, 36847 (2 June 2016).

43 On the general standard for the waiver of *Charter* rights, see *Clarkson v R*, [1986] 1 SCR 383 at 394–96; *R v Evans*, [1991] 1 SCR 869 at 892–94.

44 *Supra* note 42.

45 *Ibid* at 349.

consent, the search or seizure is by definition "reasonable" and section 8 is not infringed.[46] Conversely, if a court finds that a purported consent was unlawful, then absent any other legal authority for it, the search is unreasonable and violates section 8.[47]

To be lawful, a purported consent must be both voluntary and informed.[48] Voluntariness here has a less precise and less stringent meaning than in the context of the confessions rule.[49] Broadly speaking, a consent to search will be voluntary if it is "not the product of police oppression, coercion or other external conduct which negated the freedom to choose whether or not to allow the police to pursue the course of conduct requested."[50] In addition, the accused must have had sufficient capacity to consent. Capacity hinges on whether the accused had an "operating mind": a relatively low threshold requiring a basic understanding of language and consequences.[51]

To give an "informed" consent, the accused must have had sufficient information to allow a "meaningful" choice as to whether to permit the search.[52] This consists of several elements. First, police must inform persons "detained" within the meaning of section 10 of the *Charter* of their rights under that provision.[53] Second, they must also know that they have the right to refuse permission.[54] Though police are not obliged to give this warning, without one it will be difficult to prove that the accused knew of this right yet voluntarily decided to forego it.[55] Third, the individual must have some degree of awareness of the consequences of the search, including its investigative purpose and, "at least in cases where the person is an accused,

---

46 See e.g. *R v Borden*, [1994] 3 SCR 145 at 165 [*Borden*]; *R v Mellenthin*, [1992] 3 SCR 615 at 624–25 [*Mellenthin*]; *R v Atkinson*, 2012 ONCA 380 at para 55 [*Atkinson*]. See also Glen Luther, "Consent Search and Reasonable Expectation of Privacy: Twin Barriers to the Reasonable Protection of Privacy in Canada" (2008) 41:1 UBC L Rev 1 at 14.

47 See *R v Collins*, [1987] 1 SCR 265 at 278 (searches conducted without lawful authority are always "unreasonable" and hence always violate section 8). See also *R v Kokesch*, [1990] 3 SCR 3 at 18; *R v Stillman*, [1997] 1 SCR 607 at para 50, *R v Caslake*, [1998] 1 SCR 51 at para 12.

48 See *Wills*, *supra* note 42; PG Barton, "Searches of Premises with Consent — A Comment" (1993) 35:3 Crim LQ 376.

49 Unlike for the confessions rule, for example, a consent to search may be voluntary even if it flows from a positive inducement, such as a promise of leniency. See *Goldman v R*, [1980] 1 SCR 976 at 1006 [*Goldman*] (consent to conduct participant surveillance). On the meaning of voluntariness in the context of the confessions rule, see Penney, Rondinelli & Stribopoulos, *supra* note 17, §§4.4–4.46.

50 *Wills*, *supra* note 42 at 353–54. See also *Wills*, *ibid* at 351–52; *R v Backhouse* (2005), 194 CCC (3d) 1 at para 130 (Ont CA); *Mellenthin*, *supra* note 46 at 624–25; *Atkinson*, *supra* note 46 at para 56. See also generally *Goldman*, *ibid* at 1006 (the meaning of voluntary consent for participant surveillance under Part VI of the *Criminal Code*, *supra* note 16).

51 See e.g. *R v St Martin*, 2014 ONSC 2518 at para 37; *R v Lowrey*, 2016 ABPC 131 at para 79 [*Lowrey*]. See also generally *R v Whittle*, [1994] 2 SCR 914 at 941 (setting out the operating mind requirement for both the confessions rule and the waiver of the right to counsel under section 10(b) of the *Charter*); *R v Oickle*, 2000 SCC 38 at para 63 (the operating mind requirement for the confessions rule); *R v JA*, 2011 SCC 28 at paras 36, 43–44 (the operating mind requirement for consent to sexual touching for sexual offences); Penney, Rondinelli & Stribopoulos, *supra* note 17, §§4.20–4.23.

52 See *Borden*, *supra* note 46 at 161–62. See also *R v Arp*, [1998] 3 SCR 339 ("persons consenting must be aware of their rights and as far as possible the consequences of their consent" at para 87); *Cole*, *supra* note 25 at para 77; *Wills*, *supra* note 42 at 350; *Atkinson*, *supra* note 46 at para 56.

53 See *R v Debot*, [1989] 2 SCR 1140 at 1146–47; *Wills*, *ibid* at 351–52; *R v Calderon* (2004), 188 CCC (3d) 481 at para 85 (Ont CA).

54 See *Mellenthin*, *supra* note 46 at 624; *Atkinson*, *supra* note 46 at para 56.

55 See *R v Lewis* (1998), 38 OR (3d) 540 at 545 (CA); *R v Rutten*, 2006 SKCA 17 at paras 39, 44; *R v Luc*, 2004 SKCA 117 at para 34, leave to appeal to SCC refused, 30600 (14 April 2005); *R v Lam*, 2003 BCCA 593 at para 35; *R v Coggan* (1999), 218 NBR (2d) 369 at para 14 (QB). But see *R v Clement*, [1996] 2 SCR 289 (consent valid as the "appellant testified that he knew that the police had no right to search his car" at para 1); *R v Kennedy*, 2000 BCCA 362 (refusal to allow police to search basement was evidence that the accused knew of the right to refuse, making the initial consent valid); *R v Head (CR)* (1994), 86 WAC 121 (BCCA) (the trial judge's finding of valid consent was upheld despite a police failure to tell accused of the right to refuse).

suspect or target of the investigation," the possibility that its fruits could be used against him or her.[56] Lastly, police cannot misrepresent their authority to search. They cannot, for example, falsely suggest that they could get a warrant or otherwise lawfully search without consent.[57]

B. THIRD-PARTY CONSENT

As mentioned, third-party consent means that someone other than the accused gave police permission to search a domain over which the accused also had a reasonable expectation of privacy. Third-party consent accordingly consists of two elements: (1) a lawful consent (as detailed in Part III.A, above); (2) from a person with authority to consent in the circumstances. If both elements are present, the accused's right to be free from unreasonable search or seizure under section 8 of the *Charter* is not violated.[58]

In *Cole*, however, the Supreme Court declared that there is no third-party consent doctrine in Canada.[59] In *Cole*, a teacher stored child pornography on his employer-issued work computer. A technician performing routine maintenance found the images, copied them, and informed the principal. The principal gave the computer and data to police, who reviewed the images without first obtaining a warrant. Because the employer owned the computer and informed employees of its right to monitor usage, the prosecution argued that the accused lacked a reasonable expectation of privacy under section 8. The Supreme Court rejected that claim, observing that the employer allowed teachers to use its computers to communicate and store intimate, personal information deserving of constitutional protection.[60]

In the alternative, the prosecution argued that the employer lawfully consented to a search of its own property. The Supreme Court rejected this argument too, holding that third-party consent "could interfere with an individual's privacy interests on the basis of a consent that is *not* voluntarily given by the rights holder, and *not* necessarily based on sufficient information in his or her hands to make a meaningful choice."[61]

Does this mean that third parties can never consent to a search of a realm in which another has a reasonable expectation of privacy? The answer is clearly "no." Before and after *Cole*, courts have found that a non-accused's consent may authorize police to search places they would not otherwise be allowed to search without a warrant. But rather than saying that the third party waived the accused's section 8 rights, they have instead asked whether the third party had an independent authority to consent to the search.[62] Where two (or more) people

---

56 *Wills*, *supra* note 42 at 350, 353–54. See also *Atkinson*, *supra* note 46 at para 56; *Borden*, *supra* note 46 at 163–65.

57 See *R v O'Connor* (2002), 62 OR (3d) 263 at para 75 (CA); *R v Bergauer-Free*, 2009 ONCA 610 at paras 54–57.

58 See PG Barton, "Consent by Others to Search Your Place" (1993) 35:4 Crim LQ 441 at 442.

59 *Supra* note 25 at paras 74–79. The Court contrasted the Canadian position with that in the United States, where third-party consent is well recognized. See *Cole*, *ibid* at para 75; *United States v Matlock*, 415 US 164 (1974); *Illinois v Rodriguez*, 497 US 177 (1990).

60 *Cole*, *ibid* at paras 47, 54.

61 *Ibid* at para 78 [emphasis in original].

62 See *Wills*, *supra* note 42 at 353–54; *R v Clarke*, 2017 BCCA 453 at para 63 [*Clarke*]. If police reasonably (but wrongly) decide that a third party has the authority to consent, the consent will still be unlawful. But the reasonableness of the error will militate in favour of admitting any unconstitutionally obtained evidence under section 24(2) of the *Charter*. See *R v DiPalma*, 2008 BCCA 342 at paras 21–47; *R v Reeves*, 2017 ONCA 365 at para 71 [*Reeves*], leave to appeal to SCC granted, 37676 (14

have a shared expectation of privacy over a domain, in other words, it will not always be reasonable for one to expect that another cannot voluntarily permit police to search it.[63]

This issue arises most commonly when police seek third parties' consent to search physical spaces over which both they and the accused have expectations of privacy. Courts have repeatedly held, for example, that an accused's co-resident may consent to searches of shared or common areas of the home (but not areas used exclusively by the accused).[64] As the Ontario Court of Appeal stated in *Reeves*, "it would not be reasonable for one resident to expect that the other co-resident could never invite an agent of the state into the residence," and further, that "the other might have a legitimate interest in consenting to entry by law enforcement into common spaces from time to time."[65]

Of course, as with first-party consent, the third party's consent must be voluntary and informed. As the Court held in *Reeves*, a co-resident "would not reasonably expect police entry without the consent of another co-resident."[66] Courts have applied this principle to many types of co-residents, including spouses and other intimate partners,[67] parents,[68] and roommates.[69] They have also held that landlords, property managers, and residents may consent to searches of common areas in multi-unit buildings.[70]

December 2017), heard and reserved by SCC (17 May 2018); *R v Mercer* (1992), 7 OR (3d) 9 (CA) [*Mercer*], leave to appeal to SCC refused, 22840 (27 August 1992); *R v Brilhante* (2001), 83 CRR (2d) 349 (Ont Sup Ct J).

63 See *Reeves*, *ibid* at paras 46–52.

64 See Scott C Hutchison, *Search and Seizure Law in Canada*, vol 1 (Toronto: Carswell, 2005) (loose-leaf revision 12), ch 7(e).

65 *Reeves*, *supra* note 62 at para 48. See also Barton, *supra* note 58 ("it may be in the public interest to encourage people to come forward and expose others" at 450).

66 *Reeves*, *ibid*.

67 See *R v T (RMJ)*, 2014 MBCA 36 at paras 50–52 (a spouse lawfully consented to police entry into the home and the search of a shared area); *Reeves*, *ibid* at paras 60, 62 (a spouse lawfully consented to police entry into home); *R v Parsons*, 2017 NLCA 64 at paras 39–45 (a spouse lawfully consented to police entry and search of shared apartment); *Clarke*, *supra* note 62 at paras 49–56 (a tenant/girlfriend lawfully consented to the search of the owner/boyfriend's home but not to the private area of the garage used to store his property); *R v Meyers*, [1987] 4 WWR 624 (Alta QB) (a spouse consented to the search of shared residence); *R v Squires*, 2005 NLCA 51, leave to appeal to SCC refused, 31197 (23 March 2006) ("[a] spouse, or co-habitant of a personal residence, can authorize the police to search areas of a personal residence which are shared in common with that person's spouse or co-habitant" at para 34); *R v Hann*, 2016 CanLII 77591 at para 31 (NLPC) (a spouse lawfully consented to the search of shared residence); *R v King* (1993), 114 Nfld & PEIR 353 (NLSC (TD)) (a spouse lawfully consented to the search of shared residence).

68 See *R v Rai*, 1998 CanLII 4630 at paras 40–48 (BCSC) (a father lawfully consented to the search of his 18-year-old son's room despite the son's exclusive use as the father had maintained authority to control access); *R v W (JP)*, 1993 CarswellBC 3914 (WL Can) (BC Prov Ct (Youth Ct)) (a parent could not consent to the search of teenager's bedroom). See also *R v Wagner (WW)* (1994), 40 BCAC 70 (CA) (an aunt likely lawfully consented to search of trailer where the accused nephew also lived and paid rent, but the case was decided on the basis of section 24(2) of the *Charter*); *R v Woldrich* (1997), 122 Man R (2d) 231 (QB), aff'd (1998), 167 WAC 157 (Man CA) (the homeowner could consent to the search of all areas of home except the adult son's bedroom).

69 See also *Tymkin v Ewatski*, 2014 MBCA 4 at paras 89–94, leave to appeal to SCC refused, 35749 (26 June 2014) (an overnight guest did not have the authority to consent to police entry into the residence to arrest the accused); *R v Taylor*, [1999] YJ No 1 (QL) at paras 36–45 (Terr Ct) (a babysitter did not have the authority to consent to the search of the residence).

70 See *R v Redd*, 1999 CarswellBC 1412 (WL Can) at paras 5, 99–113 (SC), aff'd 2002 BCCA 325, leave to appeal to SCC refused, 29319 (30 January 2003) (a resident lawfully consented to police entry into the home to search for a guest's boots in the common area). But see *Mercer*, *supra* note 62 (a hotel employee could not consent to the search of a rented room); *R v Peterson*, [1993] OJ No 1598 (QL) at para 83 (Ct J (Gen Div)) (a hotel employee could not consent to the search of a rented room); *R v Blinch* (1993), 83 CCC (3d) 158 (BCCA) (a neighbour given a key by the resident for limited purposes could not consent to the entry by police); *R v Archambault*, 1993 CarswellOnt 4328 (WL Can) at paras 60–64 (Ct J (Prov Div)) (police did not determine whether the employee had the authority to consent to a search of the room at workplace).

The principle that people with shared expectations of privacy may consent to police searches also applies to personal property.[71] Such cases typically arise when police purport to obtain a third party's consent to seize, inspect, or open some type of opaque container suspected to contain evidence against the accused. Such evidence may be physical (such as drugs, weapons, or paper documents),[72] or it may consist of digital data. Courts have recognized that digital searches typically pose a greater threat to privacy than searches of non-digital property.[73] But they have suggested that third parties may consent to searches of shared devices for data that is not demarcated as belonging exclusively to the accused.[74]

While the Supreme Court held in *Cole* that the employer could not consent to a search of the teacher's computer,[75] that computer was not a shared domain in the sense discussed above. While the employer maintained the right to monitor and inspect the computer for operational purposes,[76] it did not use it to store or access its own personal information, at least not in a manner that left it indistinguishable from, or intermingled with the accused's. Imagine instead that the accused had shared the computer with another teacher and both had stored personal content on it without using separate user accounts, file folders, or other markers of exclusive, private use. In these circumstances, the Supreme Court may have found that (as with shared physical property) both teachers had authority to consent to a search.

In any case, even if courts were to prohibit (or severely restrict) third-party consent searches of shared digital devices used by an accused, the situation is very different for devices used exclusively by third parties. As I elaborate in the following section, while the sender of an electronic text communication maintains a reasonable expectation of privacy in the "conversation," even after it is received by the intended recipient, so does the recipient. And just as third parties may consent to searches of shared physical domains, they should also be able to consent to searches of shared conversations stored on their own digital devices.

IV. APPLYING CONSENT DOCTRINE TO TEXT SEARCHES

As discussed, to prove that a third party lawfully consented to a search, the prosecution must prove, firstly, that the third party had the authority to consent; and second, that the purported consent was voluntary and informed. I examine the operation of each step in the context of electronic text communications below, addressing objections and explaining why

---

71 See generally *Reeves*, *supra* note 62 at para 52.

72 See *R v Barrett*, 1995 CarswellOnt 7211 (WL Can) (Ct J (Prov Div)) (the spouse had no authority to consent to the search of a locked briefcase used exclusively by the accused).

73 See *R v Morelli*, 2010 SCC 8 at para 105; *Vu*, *supra* note 16 at paras 1–2; *Cole*, *supra* note 25 at paras 46–48; *Reeves*, *supra* note 62 at paras 54–55.

74 See *R v James* (2005), 200 CCC (3d) 549 at paras 57–58, 65 (Ont Sup Ct J) (a wife did not have the authority to consent to the search of a computer used primarily by the husband as she always asked for his permission before using it and he requested its return after marital separation). See also generally Kevin Golembiewski, "All Data Are Not Created Equal: Upholding the Fourth Amendment's Guarantees When Third Party Consent Meets the Shared Electronic Device" (2017) 56:1 Washburn LJ 35; Aaron Stanley, "The Continuing Evolution of Consent and Authority in Digital Search and Seizure" (2008) 19:1 Fordham IP Media & Ent LJ 179; John-Robert Skrabanek, "Apparent Authority in Computer Searches: Sidestepping the Fourth Amendment" (2008–2009) 97:4 Ky LJ 721.

75 *Supra* note 25 at paras 74–79. See also *R v McNeice*, 2013 BCCA 98 at para 37.

76 *Cole*, *ibid* at paras 49–63.

third-party consent doctrine largely avoids the zero-sum trap that the majority and dissenting justices in *Marakah* fell into.

A. AUTHORITY TO CONSENT

A third party's authority to consent turns on the nature of the privacy expectations that each party holds over the relevant domain. Consider first the expectation of the first party, that is, the accused sender of a text communication. As mentioned, all three of the justices writing in *Marakah* characterized the subject matter of the search as the "conversation" between sender and recipient. In her majority reasons, Chief Justice McLachlin recognized that the sender maintained a reasonable privacy expectation over the record of that conversation stored on the recipient's device.

She was correct to do so. As discussed, co-residents reasonably expect that state agents will not be able to search common areas without legal authorization or consent. The ever-present risk that a co-resident might reveal incriminating information derived from those realms does not defeat that expectation. The same should be true of electronic text conversations. As the Chief Justice emphasized in *Marakah*, granting section 8 protection to senders' messages stored on recipients' devices fosters the kind of candid and intimate communication essential to human flourishing.[77]

Without such protection, moreover, police would be largely free to ignore recipients' *Charter*-protected privacy interests in their own devices and data. Imagine that police suspect that a text conversation between A and B might reveal evidence of criminal activity. But they do not have grounds for a warrant or have any other legal authority to obtain the communications legally. So they illegally seize and obtain the conversations from both suspects' devices. Though A's section 8 right was violated and the data from his device could therefore be excluded at his trial, he would lack standing to challenge the admission of the record of the conversation obtained from B's device (and vice versa).

This is essentially what happened in *Marakah*. In his dissenting reasons, Justice Moldaver asserted that where police deliberately seek to evade *Charter* obligations in this manner, courts can employ their discretion to exclude unfairly obtained evidence under sections 7, 11(d), and 24(1) of the *Charter*.[78] The parameters of this discretion are uncertain, however, and courts have been extremely reluctant to use it to exclude reliable evidence.[79] And as Justice LaForme pointed out in his dissent in the Court of Appeal *Marakah* decision, unlike section 24(2) of the *Charter*, the trial fairness discretion is not well suited to the role of preventing *Charter* infringements and maintaining "the long-term reputation of the administration of justice."[80]

But while the Chief Justice was wise to recognize the sender's ongoing expectation of privacy in messages stored on the recipient's device, she failed to reckon with how that

---

77 *Marakah* SCC, *supra* note 1 at para 36. See also Stern, *supra* note 18 at 34–35.

78 *Marakah* SCC, *ibid* at paras 190–96, Moldaver J, dissenting.

79 See David M Paciocco & Lee Stuesser, *The Law of Evidence*, 7th ed (Toronto: Irwin Law, 2015) at 434–35.

80 *Marakah* CA, *supra* note 8 at para 177, LaForme JA, dissenting.

expectation interacts with the recipient's. Just as with shared physical spaces, courts should recognize that text conversations belong to *both* senders and recipients. As discussed, while co-residency does not defeat any one resident's expectation of privacy over shared living spaces, any co-resident may voluntarily consent to searches of those areas. As noted in *Reeves*, a co-resident will often have a "legitimate interest" in consenting to such searches.[81] The same should be true of text communications. Indeed, while it is sometimes difficult to decide whether residential spaces are shared or exclusive, received text communications are always shared between the parties.[82] The law should therefore permit third parties, including victims of and witnesses to criminal activity, to consent to searches of their devices for incriminating messages sent to them. Such a capacity would further public safety and crime control without unduly diminishing the privacy of electronic communications.

This conclusion is buttressed by Part VI of the *Criminal Code*, which regulates the interception and recording of private communications. Section 184 makes it an offence for anyone to intercept a private communication, subject to certain exceptions. Most pertinent to this article, this prohibition does not apply to a party to a private communication, whether oral or text-based.[83] A party to a private, oral conversation may consequently record it, even surreptitiously, without committing an offence. Why then would the law forbid a party from voluntarily disclosing to police a text conversation that the sender knew would be recorded?

In *Duarte*, Justice La Forest famously rejected the "risk analysis" favoured in the American jurisprudence, holding that there was a vast difference between the risk that confidants will disclose private communications and the risk that the state will covertly intercept and record them.[84] This danger does not arise, however, from a private citizen's voluntary, *ex post* decision to disclose an inherently recordable conversation that he or she was privy to.[85]

Denying recipients the authority to consent would also unjustifiably thwart law enforcement. Complainants and witnesses in harassment, sexual violence, and domestic violence cases commonly provide text communications to police.[86] If they were prohibited from disclosing these messages on consent, police would generally need judicial authorization to obtain them.[87] This would require convincing a justice that there were

---

81 *Supra* note 62 at para 48.

82 See *Lowrey*, *supra* note 51 at paras 62, 82–85.

83 In *Duarte*, *supra* note 31, the Supreme Court of Canada held that such "participant" or "first-party" intercepts invade a reasonable expectation of privacy and violate section 8 of the *Charter* when police conduct them without legal authorization. Parliament subsequently amended Part VI to permit police to such surveillance with a warrant. See *Criminal Code*, *supra* note 16, s 184.2. See also the discussion in Part V.A, below.

84 *Duarte*, *ibid* at 44.

85 See Stern, *supra* note 18 at 43–44.

86 See e.g. *R v Wenc*, 2009 ABCA 328 at paras 2–10 (criminal harassment); *R v Danielson*, 2013 ABPC 26 at paras 10–22 (child luring); *Lowrey*, *supra* note 51 at paras 1, 9 (child luring); *R v Aguas*, 2015 ONSC 3462 at para 11 (sexual assault and voyeurism); *R v Racco*, 2013 ONSC 1517 at para 28 (sexual assault); *R v KMM*, 2012 SKQB 297 at para 10 (sexual assault); *R v Polsom*, 2011 ABPC 390 at para 21 (sexual assault); *R v Stanley*, [2014] OJ No 6378 (QL) at paras 5, 7 (Ct J) (sexual interference, invitation to sexual touching, and child luring); *R v Green*, 2015 ONCJ 265 at para 4 (uttering threats, assault, and harassment); *R v Ganong*, 2013 CarswellOnt 12187 (WL Can) (Sup Ct J) (sexual assault, sexual touching, and invitation to sexual touching).

87 Some commentators have noted that there is no "state action," and hence no possibility of a *Charter* violation, when private citizens turn over information to police. See e.g. Stern, *supra* note 18 at 43; Chris De Sa, "*R. v. Marakah*: The Complexities of Standing in the Context of Sent Text Messages" (20 February 2017), online: Social Science Research Network <https://ssrn.com/abstract=3069932>. This

probable grounds to believe that the messages would reveal evidence of a specific crime.[88] But if complainants or witnesses tell police that they received incriminating texts, how are police to confirm their evidentiary significance without looking at them? And if recipients were to read the relevant messages to police to provide probable grounds, how would this differ substantively from police looking at the messages themselves? Further, while texts may not always provide grounds for a warrant, they may still help to advance the investigation, for example by identifying or eliminating suspects or providing grounds for less onerous authorizations, such as those requiring reasonable suspicion instead of probable grounds.[89]

Some jurists have suggested an alternative solution: exempting communications constituting an element of an offence, such as uttering threats, from section 8 protection.[90] On this view, senders of such communications cannot reasonably expect them to remain private.[91]

There are several problems with this approach. First (and most importantly), the exception is too narrow. As explained immediately above, many text communications provide evidence of an offence or other valuable investigative information without being criminal in themselves.

Second, the proposal violates a cardinal principle of section 8 jurisprudence: state intrusions onto privacy must be assessed *ex ante*, not *ex post*.[92] In other words, in deciding whether a person enjoys a reasonable expectation of privacy in a domain, courts must not be influenced by *ex post* knowledge that it was used for criminal purposes. They may consider only the types of activities and information generally associated with that domain.

Third, since police will not always be certain *ex ante* that the communication constitutes a crime, they will often err in deciding whether they can search without a warrant. In some cases, they may decide not to search, incorrectly fearing that the exception did not apply. In others, they may decide to search under the incorrect belief that the exception did apply. In the former case, potentially valuable, admissible evidence might never become available to the prosecution. In the second, probative evidence could be excluded under section 24(2) for violating section 8 of the *Charter*. And if the exception were recast as applying whenever

may be the case, for example, where a third party gives text communications directly to police. But the *Charter* will likely apply if police must do something to access the information (for example, by manipulating a digital device), even if a third party has voluntarily facilitated that access. See *R v Buhay*, 2003 SCC 30 at paras 33–34; *Cole*, *supra* note 25 at paras 67–73.

88 See *Criminal Code*, *supra* note 16, s 487 (search warrant for "building, receptacle or place"), s 487.014 (production order for document).

89 See e.g. *ibid*, s 492.1 (warrant for "tracking devices"), s 492.2 (warrant for "transmission data"), s 487.012 (preservation demand for computer data), s 487.013 (preservation order for computer data), s 487.015 (production order for transmission data identifying person or device), s 487.016 (production order for transmission data), s 487.017 (production order for tracking data).

90 See *Pelucco*, *supra* note 2 at paras 47–48, 61; *Marakah* CA, *supra* note 8 at para 171, LaForme JA, dissenting.

91 See *Pelucco*, *ibid* ("a person who threatens another has no right to expect that the person who has been threatened will keep the threat private" at para 61); *Marakah* CA, *ibid* ("the fact that the sender of the text messages in *Sandhu* was threatening the recipient is a part of the totality of the circumstances that must be considered when evaluating an assertion of a reasonable expectation of privacy" at para 171, LaForme JA, dissenting).

92 See *R v Wong*, [1990] 3 SCR 36 at 49–50 [*Wong*]; *Spencer*, *supra* note 23 at para 36; *Patrick*, *supra* note 25 at para 32.

police had probable grounds to believe that the communication was criminal, it would be little different from a rule requiring warrants in all cases.

It makes more sense to resolve "threat" and analogous cases with the consent doctrine. As elaborated in Part IV.B, immediately below, it should generally be easy for police to make accurate, *ex ante* determinations of recipients' capacity and willingness to consent. If police make the proper inquiries and accurately record the recipient's consent, the search will very likely be lawful and the acquired communication admissible, even if the communication does not constitute an offence. Requiring police to obtain a warrant to examine text communications despite such a consent would erode their ability to fight crime without enhancing communications privacy in any meaningful way.

B. VOLUNTARY AND INFORMED

A lawful third-party consent requires not only an authority to consent, but also a voluntary and informed decision to do so. In his dissent in *Marakah*, Justice Moldaver warned that even if text message recipients have the authority to consent, it would often be too difficult to obtain and impose needless harm on victims.[93] The elements of an informed and voluntary consent, he asserted, are so onerous that police would likely "seek judicial authorizations in most cases out of an abundance of caution to take basic investigative steps such as obtaining records of electronic communications between witnesses and accused persons."[94] The process of obtaining consent, he added, could expose "children or other vulnerable witnesses to cross-examination about consent given to the police to search their phones or other devices for private communications that may involve threats or sexual predation."[95]

These concerns are largely unwarranted. Proving that a text recipient's purported consent was voluntary and informed should not be nearly as difficult as Justice Moldaver suggests. While the "voluntary and informed" prerequisite applies to both first-party and third-party consent claims, the two types are vastly different in practice. In first-party cases, the state and consenting party are usually adversaries, as when police seek criminal suspects' permission to search for evidence to incriminate them. In this scenario, the potential for coercion is manifest. When the search is likely to reveal incriminating information, any consent will run against the suspect's best interests. Courts have accordingly imposed rigorous requirements on the prosecution to prove that the consent was truly voluntary and informed.[96]

In most third-party consent scenarios, in contrast, the state and consenting party are on the same side (or at least not adversaries). This is especially true of electronic text cases.[97]

---

93 *Supra* note 1 at paras 182–84, Moldaver J, dissenting.

94 *Ibid* at para 184.

95 *Ibid*.

96 See Luther, *supra* note 46 ("[t]he Supreme Court of Canada has generally applied a stringent waiver test where the Crown contends that an accused has yielded a constitutional right in the course of a police investigation" at 5).

97 In shared residence cases, in contrast, the third party purporting to consent is often a family member or friend of the suspect and could therefore be in a quasi-adversarial relationship with police. See e.g. *R v Young* (1987), 65 Nfld & PEIR 357 (NLSC (TD)) (the accused's mother did not validly consent to the search of the shared residence as she was not aware of the right to refuse); *R v Guiboche*, 2004 MBCA 16 at para 59, leave to appeal to SCC refused, 30272 (26 August 2004) (a parent homeowner lawfully consented to the police entry to arrest the accused and conduct a search). See also *R v Adams* (2001), 203 DLR (4th) 290 (Ont CA) (the apparent consent of a superintendent to search the shared laundry

Consider the decision in *Lowrey*.[98] There, the accused was charged with "child luring" after sending private Facebook messages to a 14-year-old complainant. After the complainant and her mother signed a written consent form, police used her Facebook account to copy the messages. In a decision rendered before the Supreme Court released *Marakah*, Judge Rosborough concluded that the accused lacked a reasonable expectation of privacy in the received messages.[99] In the alternative, he found that the complainant lawfully consented to the search.[100] He wrote:

> Where the victim of a crime engages the police in this fashion, it is somewhat artificial to inquire whether that victim "consented" to the police undertaking an investigation. Not only can Angela L. be said to have *consented* to Cpl. Bristow's actions, those actions were undertaken *at Angela L.'s request*. This is not a case where police seek to have a suspected criminal agree to incriminate himself. And different considerations must apply.[101]

He nonetheless went on to apply the *Wills* test for first-party consent, finding that it was informed and voluntary even though the complainant was cognitively challenged.[102]

This is an eminently sensible approach. While the prosecution properly bears the burden of proving that any waiver of section 8 is voluntary and informed, courts must be sensitive to factual circumstances, including the third party's own autonomy, security, and privacy interests.[103] For complainants and other prosecution witnesses, it should rarely be difficult to obtain a lawful consent. Nor should the requirement to prove consent cause undue harm. Victims and witnesses will normally be required to testify about the same (potentially sensitive) matters at the trial proper. Asking them to relate the details of their consent during a *Charter voir dire* is unlikely to cause them significant additional harm.

V. PROSPECTIVE SURVEILLANCE FROM RECIPIENTS' DEVICES

The discussion so far has been about *retrospective* consent searches for electronic text on recipients' devices. In such cases, the individual agrees to give police access to texts received before the consent was given. But recipients may also allow police to *prospectively* monitor and record incoming messages in hopes of obtaining incriminating information. Such messages are recorded on the recipient's device (and almost always sent) after the consent has been granted. In some cases, police may even take control of the device and send messages posing as the intended recipient. The question raised here is whether this kind of warrantless prospective surveillance is, or should be, legally permissible.

---

room was vitiated by trickery).

98 *Supra* note 51.

99 *Ibid* at paras 59–70. This aspect of the decision has likely been overtaken by *Marakah* SCC, *supra* note 1.

100 *Lowrey*, *ibid* at paras 71–85.

101 *Ibid* at para 73 [emphasis in original]. See also *ibid* at para 78 (questioning whether the high standard for waiver should apply to victims seeking police assistance).

102 *Ibid* at paras 74–79.

103 See Stern, *supra* note 18 at 43–44 (arguing that third parties' voluntary decisions to disclose text communications to police do not engage senders' reasonable expectations of privacy). See also generally Orin S Kerr, "An Economic Understanding of Search and Seizure Law" (2016) 164:3 U Penn L Rev 591 at 607, 621 (from an economic perspective, consent searches impose relatively small external costs on society).

The answer turns on whether the prospective acquisition of text from a recipient's device (with or without the recipient's consent) is captured by Part VI of the *Criminal Code*, which governs the interception of electronic communications. For many years, Part VI applied only to "third-party" interceptions, commonly known as "wiretaps." A third-party interception involves the prospective acquisition of private communications between two or more parties, none of whom are aware of the interception. As mentioned, Part VI criminalizes such interceptions, subject to several exceptions, including police acting under judicial authorization.[104] But the criminal prohibition, and the concomitant requirement for police to obtain an authorization, did not apply to "first-party" interceptions, that is, the prospective acquisition of private communications where one party was aware of the interception.

The Supreme Court held in *Duarte*, however, that first-party interceptions invade a reasonable expectation of privacy and that the failure to obtain judicial preauthorization violates section 8 of the *Charter*.[105] Parliament responded by enacting section 184.2 of the *Criminal Code*, which permits first-party interceptions with authorization on probable grounds. That provision states that a person may

> intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where either the originator of the private communication or the person intended by the originator to receive it has consented to the interception and an authorization has been obtained pursuant to subsection (3).[106]

Police must accordingly obtain a section 184.2 authorization if each of the following elements is present: (1) either the originator or intended recipient of the communication consents to the surveillance; (2) the information acquired constitutes a "private communication"; and (3) police "intercept" that communication. I deal with each of these issues in turn, below.

A. CONSENT

The issue of consent is straightforward. If police have obtained an intended recipient's voluntary and informed permission to acquire incoming messages, that person will have "consented to the interception" and police can apply for an authorization. In addition, if police lawfully acquire the intended recipient's device without consent, they may still obtain a participant authorization in their capacity as the "originator" of any messages they send from the intended recipient's device. In either case, the surveillance will be considered "first-party" (and potentially subject to section 184.2) and not "third-party."

---

104 *Criminal Code*, *supra* note 16, s 184.
105 *Supra* note 31.
106 *Criminal Code*, *supra* note 16, s 184.2(1). See also the discussion in Part V, below.

B. PRIVATE COMMUNICATION

The *Criminal Code* makes it clear that section 184.2 encompasses both oral and electronic text communications.[107] The only question is whether received text communications are "private." This turns on whether senders have a reasonable expectation of privacy over messages obtained from recipients' devices. As discussed, the Supreme Court decided in *Marakah* that the answer is generally "yes."[108] Certainly, any text communication sent to a specific, known recipient (or small group of recipients) will constitute a private communication under Part VI.

Some courts have concluded, however, that messages sent to anonymous or pseudonymous strangers (typically undercover police in child pornography and sexual exploitation investigations) may not attract a reasonable expectation of privacy.[109] In *Mills*, for example, the Newfoundland and Labrador Court of Appeal found that the accused did not have a reasonable expectation of privacy in messages he sent to a person whom he believed was a 14-year-old girl.[110] The recipient was in fact a fictitious Facebook profile created by police to lure persons seeking illegal sexual contact with minors.[111] The Court concluded as follows:

> Mr. Mills was using electronic social media to communicate and share information with a person he did not know and whose identity he could not confirm. On an objective analysis, as the sender of such communications, Mr. Mills must have known that he lost control over any expectation of confidentiality that he appears to have hoped would be exercised by the recipient of the messages. He took a risk when he voluntarily communicated with someone he did not know, a person he was not in a position to trust. Any subjective expectation of privacy Mr. Mills may have had was not objectively reasonable.[112]

---

107 *Criminal Code*, *ibid* defines "private communication" at section 183 [emphasis added]:

> any oral communication, *or any telecommunication*, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it.

"Telecommunication" is defined in section 35(1) of the *Interpretation Act*, RSC 1985, c I-21, as "the emission, transmission or reception of signs, signals, *writing*, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system" [emphasis added].

108 *Marakah* SCC, *supra* note 1.

109 See e.g. *Mills* CA, *supra* note 20 at para 23; *R v Graff*, 2015 ABQB 415 at paras 57–66 [*Graff*]; *R v Merritt*, 2017 ONSC 1648 at paras 55–104 [*Merritt*]; *R v Ghotra*, [2015] OJ No 7253 (QL) at paras 100–31 (Sup Ct J) [*Ghotra*]; *R v Allen*, 2017 ONSC 1712 at paras 54–63 [*Allen*]; *R v NJS*, 2014 BCSC 2658 at paras 65–71 [*NJS*].

110 *Mills* CA, *ibid*.

111 *Ibid* at paras 2–4.

112 *Ibid* at para 23. See also *Graff*, *supra* note 109 at para 63:

> In sum, the Applicant sent highly personal information over the internet to a complete stranger, in the absence of any invitation to send such information, and without taking any reasonable steps to ascertain the identity of the recipient, to ensure his own anonymity, or to ensure any confidentiality with respect to the information he sent.

Merritt, *supra* note 109 (accused persons "were communicating with someone who was essentially a stranger" at para 82); *Ghotra*, *supra* note 109 at para 130:

> By communicating with a stranger [the accused] potentially exposed his communications to the public, to a sector of the public or at the very least, there was a realistic potential the recipient would expose the communications to others or make a permanent record of them beyond the conversations being accessible in her computer for a significant period of time.

NJS, *supra* note 109 ("emails that have been sent and received between individuals who are unknown to each other do not fall within the definition of electronic communications" at para 70).

The notion that communicating with strangers attracts no reasonable expectation of privacy is difficult to square with Supreme Court jurisprudence, however. In *Wong*, the Supreme Court rejected the lower Court's view that a person who invited strangers to a hotel room could not reasonably expect that police would not use a hidden video camera to monitor activity in the room.[113] Writing for the majority, Justice La Forest rebuked the Court below for applying the same "risk analysis" that the Supreme Court had rejected in *Duarte*.[114] Strangers who meet in hotel rooms to engage in matters of common interest, he noted, do not "tacitly consent to allowing agents of the state unfettered discretion to make a permanent electronic recording of the proceedings."[115]

The Supreme Court has also recognized that anonymity plays an important role in protecting privacy on the internet. In *Spencer*, it found that people have a reasonable expectation of privacy in the "subscriber" information used to determine the identity of anonymous internet users.[116] Anonymity, Justice Cromwell reasoned, gives people the freedom to pursue personal growth and fulfillment without fear of pervasive online surveillance.[117]

If people reasonably expect privacy in convening with strangers in hotel rooms and using the internet anonymously, they should expect the same when they send text communications without certain knowledge of the recipient's real identity or purpose. This position accords with the "normative" approach to section 8 interpretation that conceives the provision as protecting individuals against excessive state surveillance, rather than a "descriptive" one that conditions constitutional protection on the practical availability of privacy on the ground.[118]

Further, if courts were to recognize a "stranger" exception to *Marakah*, how would they decide whether recipients were sufficiently unknown to the sender to preclude an expectation of privacy? Is it unreasonable to expect protection against state surveillance if one does not know a recipient's full, true name? As noted in *Spencer*, anonymous identities are ubiquitous online.[119] Conditioning section 8 protection on knowledge of the recipient's real name (or any other marker of identity) would leave many digital conversations vulnerable to unregulated surveillance. Surely there have been countless first-party interceptions of oral communications where the consenting parties were essentially "strangers" to the targets, for example where targets had not previously interacted with consenting parties or where targets reasonably assumed that consenting parties would not use their real or full names.[120] If these conversations are private communications under section 184.2 (as they surely are), analogous text conversations should be too.

---

113 *Wong*, *supra* note 92.
114 *Ibid* at 49, 51.
115 *Ibid* at 51.
116 *Supra* note 23.
117 *Ibid* at paras 41–48.
118 See *Spencer*, *ibid* at para 18; *Wong*, *supra* note 92 at 46; *Tessling*, *supra* note 23 at para 42; *Patrick*, *supra* note 25 at para 14; *Goodwin v British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46 at para 48; Renee M Pomerance, "Flirting with Frankenstein: The Battle Between Privacy and Our Technological Monsters" (2016) 20:2 Can Crim L Rev 149 at 159–60; Amsterdam, *supra* note 3 at 402.
119 *Spencer*, *ibid* at para 48. See also *R v Ward*, 2012 ONCA 660 at para 71.
120 Notably, I was unable to find any reported decisions where a court found that a surreptitious interception or recording of an oral conversation was not a "private communication" because the consenting party was insufficiently known to the target.

In any case, the "stranger" issue rarely arises when text recipients voluntarily cede control of their devices to police. In all but rare cases, the sender will know the intended recipient's real identity and the messages will therefore unequivocally be "private communications" under Part VI. It should not matter that, unknown to the sender, police gained access to the recipient's device (and may even be posing as the recipient to induce further communications from the sender). Just as oral in-person and telecommunications are still "private communications" when made to undercover police or civilian police informants, so are text messages sent to devices that police have coopted.

C. INTERCEPT

The final question is whether police "intercept" text communications within the meaning of section 184.2 when they prospectively obtain them from recipients' devices. There is no question that police intercept a message if they acquire it "in transit," that is, before it is stored in anything other than short-term memory in the transmission network.[121] It is also clear that police require Part VI authorizations to prospectively acquire messages copied to long-term memory by a service provider. In *Telus*, the Supreme Court had to decide whether police could prospectively obtain text messages from a service provider using a "general warrant" under section 487.01 of the *Criminal Code*. Such warrants cannot be issued if there is another, more specific provision authorizing the intrusion.[122] Three of the five majority justices, in an opinion authored by Justice Abella, held that the intrusion constituted a Part VI "interception."[123] The remaining two, speaking through Justice Moldaver, declined to decide whether it was an interception, preferring to hold that it was "substantively equivalent" to one and thus could not be authorized by section 487.01.[124]

Despite Justice Moldaver's equivocation, *Telus* can only be interpreted as requiring Part VI authorizations for the prospective acquisition of text communications from a third-party service provider, whether the communications are immediately accessible to police (as with traditional wiretaps) or are forwarded to them on an ongoing basis (as in *Telus*).[125] But the Supreme Court in *Telus* did not decide whether the same result would hold if police prospectively obtain messages from recipients' devices, with or without consent.

Most courts that have considered the question have concluded that it does not, reasoning that since police did not capture the messages in transit from the sender's device to the recipient's, they were not intercepted within the meaning of Part VI.[126] On this view, the fact

---

121 See *Telus*, *supra* note 6 ("[h]ad the police acquired the same private communications directly from the transmission stream, instead of from the stored copies, the Crown concedes that a Part VI authorization would be required" at para 40, Abella J). Note, however, that police do not need Part VI authorizations to obtain historical text messages from service providers. That is, messages already in storage at the time that police became authorized to obtain them. These communications may be obtained with ordinary search warrants or production orders. See *Jones*, *supra* note 6 at paras 59–81; *R v Belcourt*, 2015 BCCA 126 at paras 41–55 [*Belcourt*].

122 *Criminal Code*, *supra* note 16, s 487.01(1)(c).

123 *Telus*, *supra* note 6 at paras 12, 33–45, Abella J.

124 *Ibid* at paras 52, 65–77, Moldaver J.

125 See *Pelucco*, *supra* note 2 at para 33.

126 See *Blais c R*, 2017 QCCA 1774 [*Blais*] (police seized the arrestee's device and used it to text the accused); *Pelucco*, *ibid* (police seized the arrestee's device and used it to text the accused); *R v Beairsto*, 2018 ABCA 118 at para 25 [*Beairsto* CA] (police seized the arrestee's device and used it to text the accused); *R c Noël*, 2013 QCCQ 15544 [*Noël*] (police seized the arrestee's device and used it to text the accused). See also *Mills* CA, *supra* note 20 at paras 11–13 (police exchanged private messages with the

that police gained access to the recipient's device before the message was sent (and may even have solicited the message posing as the recipient) is immaterial: there is no interception unless police access a message before it is copied to the recipient's device.[127]

These decisions, however, cannot be reconciled with the Supreme Court's jurisprudence on text messages and consent surveillance. To begin, *Marakah* has ended the debate over whether senders retain a privacy expectation in communications obtained from recipients' devices (they do). To the extent that the "no intercept" decisions rely on the contrary position, they can be disregarded.[128]

Further, if senders have a reasonable expectation of privacy over historical text messages retrieved from recipients' devices, their expectation of privacy over future messages should be even stronger. As Justice Moldaver noted in his dissent in *Marakah*, the recipient there exercised exclusive control over the messages before police seized his device, giving him "complete autonomy to disclose them to anyone, at any time, and for any purpose."[129] As mentioned, this led Justice Moldaver to reject the majority's view that the sender maintained a reasonable expectation of privacy over the messages. But if police had intercepted those same messages, he wrote, the sender would have been protected. The sender "reasonably assumed that, in conversing with Mr. Winchester through text messaging, he was communicating *only* to Mr. Winchester," reasonably expecting that his messages "would not be clandestinely intercepted."[130] This expectation is violated regardless of whether the messages are captured in transit or after they are received on a device that police have covertly acquired. In each case, the police intercede and obtain the messages, without the sender's knowledge, on an ongoing basis.

Denying Part VI protection in this scenario also conflicts with *Telus*. The definition of "intercept" is broad and inclusive, Justice Abella wrote, and should not be constricted by

---

accused while posing as a fictitious underage girl); *Allen*, *supra* note 109 at paras 54–63 (police exchanged private messages with the accused while posing as a fictitious underage girl); *Ghotra*, *supra* note 109 at paras 100–31 (police exchanged private messages with the accused while posing as a fictitious underage girl); *Graff*, *supra* note 109 at paras 57–66 (police exchanged private messages with the accused while posing as a fictitious underage girl); *NJS*, *supra* note 109 at paras 65–71 (undercover police posing as a pimp for underage prostitutes exchanged emails with the accused); *R v Shaw*, 2017 NLTD(G) 87 at paras 30–31 (undercover police posing as a criminal exchanged text messages with the accused). See also *R v McQueen*, [1975] 6 WWR 604 (Alta CA) (police answered the landline phone while executing a warrant and impersonated a resident in conversing with the accused caller); *R v Singh* (1998), 127 CCC (3d) 429 (BCCA) (police answered the landline phone while executing a warrant and impersonated a resident in conversing with the accused caller); *Lebeau c R*, [1977] CA 419 (Que) (no interception where police answered the landline phone in the accused's room and conversed with callers in guise of the accused taking illegal bets); *R v Ramsum*, 2003 ABQB 45 at paras 28–29 (no interception when police answered the arrestee's mobile phone and impersonated him); *R c Bonneau*, 2009 QCCS 6556 [*Bonneau*] (no interception when police answered the arrestee's mobile phone and impersonated him); *R v Perri*, 2007 ABPC 229 (no interception when police answered the arrestee's mobile phone and impersonated him).

127 See *Blais*, *ibid* at paras 19–21; *Pelucco*, *ibid* at para 33; *Bonneau*, *ibid* at paras 29–30; *Noël*, *ibid* at para 53; *Mills* CA, *ibid* at paras 12–16; *Beairsto* CA, *ibid* at para 25.

128 See *Noël*, *ibid* at paras 35–50; *Mills* CA, *ibid* at para 23; *Allen*, *supra* note 109 at paras 45–46, 53. See also *R v Thompson*, 2013 ONSC 4624 at para 43. The question of whether texts sent to a stranger attract a reasonable expectation of privacy is discussed in Part V.B, above.

129 *Marakah* SCC, *supra* note 1 at para 145.

130 *Ibid* at para 146 [emphasis in original]. See also *Belcourt*, *supra* note 121 at paras 45–47.

"technical differences" between various modes of acquisition.[131] Echoing *Wong*, she stressed that Part VI must be interpreted in light of section 8 of the *Charter*, "which in turn must remain aligned with technological developments."[132] In concluding that interceptions need not "occur simultaneously with the making of the communication itself," she noted that copies of electronic text often exist in multiple locations and may accordingly be intercepted "more than once from different sources."[133]

And as both Justice Abella and Justice Moldaver observed in *Telus*, there is a critical difference between police obtaining messages already received by the intended recipient and obtaining future communications.[134] The latter represents a graver threat to privacy than the former and is accordingly governed by the more stringent conditions set out in Part VI of the *Criminal Code*.[135]

The "no intercept" decisions are also difficult to square with *Duarte* and the use of section 184.2 of the *Criminal Code* to intercept oral communications. As discussed, in *Duarte* the Supreme Court interpreted section 8 as requiring police to obtain judicial authorization to conduct first-party, participant surveillance, that is, to intercept a private conversation with one party's consent. This caused Parliament to enact section 184.2, which provides for such an authorization on less onerous terms than a conventional, third-party wiretap authorization.[136]

Traditionally, police have used section 184.2 to surreptitiously intercept and record oral conversations between a suspect and either an undercover police officer or civilian informer.[137] But obtaining prospective text communications from a recipient's device is a substantively equivalent form of surveillance.[138] It is no less a first-party, participant

---

131 *Telus*, *supra* note 6 at paras 3–5, 24–25. See also *Telus*, *ibid* (stressing the need to "assess the substance of the police investigative technique, not merely its formal trappings" and warning against drawing "an artificial and unrealistic distinction" between simultaneous acquisition of text messages and prospective acquisition of messages from memory at paras 62, 68, Moldaver J); *Criminal Code*, *supra* note 16 (intercept "includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof," s 183).

132 *Telus*, *ibid* at para 33, Abella J. See also *ibid* ("[a] technical approach to 'intercept' would essentially render Part VI irrelevant to the protection of the right to privacy in new, electronic and text-based communications technologies, which generate and store copies of private communications as part of the transmission process" at para 33).

133 *Ibid* at paras 34, 39.

134 *Ibid* at para 42, Abella J, para 67, Moldaver J. See also *Jones*, *supra* note 6 ("[b]ased on its plain meaning, interception suggests a prospective concept of authorization relating to communications not yet in existence" at para 69).

135 *Telus*, *ibid* at para 42, Abella J, paras 73–76, Moldaver J.

136 See *Criminal Code*, *supra* note 16, s 185. A judge may issue an authorization under section 184.2(3) if:

> (a) there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed;
> (b) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; and
> (c) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (a) will be obtained through the interception sought.

See also generally *R v Pires; R v Lising*, 2005 SCC 66 at paras 8, 21, 30, 50 [*Pires; Lising*]; *R v Bordage* (2000), 146 CCC (3d) 549 at paras 19–20 (Que CA) [*Bordage*].

137 See e.g. *Pires; Lising*, *ibid*; *R v Della Penna*, 2012 BCCA 3; *Bordage*, *ibid*.

138 See *Mills v R*, 2013 CanLII 74953 at paras 22, 44 (NLPC) [*Mills* Trial], rev'd *Mills* CA, *supra* note 20. See also *R v Kwok*, 2008 CarswellOnt 2634 (WL Can) at para 22 (Ct J) (police posing as a person interested in trading child pornography online required section 184.2 authorization to record private chat communications with the accused); *R v Ley*, 2014 BCSC 2018, at paras 39–50 (the use of video cameras in a casino to read a suspect's incoming text messages constitutes an interception requiring third-party authorization under Part VI).

interception than a police agent wearing a "wire" or recording a telephone conversation. In each case, senders who think that they are conversing exclusively with specific, intended recipients are in fact conversing with agents of the state.

Attempts to distinguish text interception from *Duarte* have been unconvincing. In *R. v. Beairsto*, for example, the trial Court asserted that the Supreme Court's concern in *Duarte* was to prevent conversations from being clandestinely "memorialized through a permanent electronic record."[139] But since the accused knew that his text messages would be recorded on the recipient's device, this concern did not materialize. "Mr. Beairsto's misapprehension," it reasoned, "related only to the identity of the recipient."[140] The Court accordingly characterized his claim as relating to unfair trickery, not unjustified surveillance.[141]

This reasoning misses the point of *Duarte*. As Justice La Forest noted, participant surveillance triggers section 8 protection because it gives the *state* access to what was intended to be a private conversation between *private* citizens. Though the following passage has been quoted many times, it bears repeating again here:

> The rationale for regulating the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it … has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. No set of laws could immunize us from that risk. Rather, the regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.[142]

The fact that police do not require any technological intervention to obtain text communications from recipients' devices does not change this calculus. As the Supreme Court observed in *Telus*, *Marakah*, and *Jones*, text communications are no less conversational than oral ones, with the former increasingly displacing the latter in the digital era.[143] And just like authors of text, speakers cannot prevent hearers from disseminating their speech to others, through either human memory or (more rarely) electronic recording. If it is faulty "risk analysis" to deny privacy protection for the former, it is equally so for the latter.[144]

---

139 *R v Beairsto*, 2016 ABQB 216 at para 60 [*Beairsto* Trial], aff'd *Beairsto* CA, *supra* note 126.

140 *Beairsto* Trial, *ibid*. This reasoning was echoed by the Court of Appeal: *Beairsto* CA, *ibid* ("[s]imply put, as I see it, deception does not amount to an interception" at para 24). See also *NJS*, *supra* note 109 at paras 56–57.

141 *Beairsto* Trial, *ibid* at paras 61, 64–65. The Court subsequently rejected the argument that the police conduct was so unfair as to constitute an abuse of process (at paras 69–70).

142 *Duarte*, *supra* note 31 at 43–44.

143 *Marakah* SCC, *supra* note 1 at para 17, McLachlin CJC, para 87, Rowe J, concurring, paras 94, 111 Moldaver J, dissenting. See also *Jones*, *supra* note 6 at para 14; *Telus*, *supra* note 6 at para 5, Abella J.

144 See *Duarte*, *supra* note 31 at 47–48, 51; *R v Fliss*, 2002 SCC 16 (noting that *Duarte* "established the principle that the secret recording of a conversation by one of the participants who is an agent of the state" violates section 8 as it "annihilates the very important right to choose the range of our listeners" at para 47). See also Stern, *supra* note 18 at 31.

Recall that the Supreme Court held in *Telus* that requiring the service provider to continuously forward stored messages to police was either a Part VI interception or substantively equivalent to one. But unlike a traditional wiretap, police did not themselves use (or cause the provider to use) any intervening technical tool to capture the messages. Instead, the provider had already copied and stored them (along with all other text messages sent or received by its customers) without state involvement. Police simply obtained a court order compelling the provider to prospectively hand over messages that it would have copied for business purposes in any case.

As discussed, the Supreme Court found that the order used (a general warrant under section 487.01) was not available in the circumstances. But police could have acquired the same messages with an intercept authorization under section 185 of the *Criminal Code*.[145] The fact that communications obtained under such authorizations are typically acquired by a different technical process is immaterial.[146] Whether under an (unlawful) section 487.01 warrant or a section 185 authorization, the provider prospectively discloses, for a specified period, any text messages sent to or received by the target using its network.

It is true that when police obtain incoming messages from recipients' devices, they do not normally require cooperation from service providers. But why should this make any difference? Consider a person who voluntarily gives police her device. Police reasonably believe that someone will send her incriminating text messages in the future, but they will not be retrievable from the device for technical or security reasons.[147] They accordingly seek an authorization to obtain the messages from the service provider under Part VI (as *Telus* requires). Since they have the intended recipient's consent to obtain the messages, police apply for a participant authorization under section 184.2. Though participant interceptions do not typically require third-party assistance, nothing in section 184.2 precludes it. Indeed, section 184.2(5) specifically empowers the authorizing judge to issue an ancillary order compelling a third party to provide any assistance reasonably required to "give effect to the authorization or warrant."[148] If police need a section 184.2 participant authorization to prospectively acquire text messages from a service provider, surely the same type of authorization is needed to obtain *the very same messages* from the recipient's device.

Nor should anything be made of the fact that Part VI refers to interception by means of an "electro-magnetic, acoustic, mechanical or other device."[149] The *Criminal Code* defines that phrase, in the relevant part, as "any device or apparatus that is used or is capable of

---

145 See *Telus*, *supra* note 6 at para 73.

146 See *ibid* at paras 40–41, Abella J, para 68, Moldaver J.

147 See e.g. Kim Zetter, "Apple's FBI Battle Is Complicated. Here's What's Really Going On," *Wired* (18 February 2016), online: <https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/>.

148 *Criminal Code*, *supra* note 16, s 184.2(5) [emphasis added]:

> A judge who gives an authorization under this section may, at the same time, issue a warrant or make an order under any of sections 487, 487.01, 487.014 to 487.018, *487.02*, 492.1 and 492.2 if the judge is of the opinion that the requested warrant or order is *related to the execution of the authorization*.

Criminal Code, *ibid*, s 487.02 [emphasis added]:

> If an authorization is given under section *184.2*, 184.3, 186 or 188 or a warrant is issued under this Act, the judge or justice who gives the authorization or issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the authorization or warrant.

149 See e.g. *ibid*, ss 184(1), 184.1(1), 184.2(1), 184.4.

being used to intercept a private communication."[150] On a plain reading, the recipient's device (after it has been appropriated by police) is one that can be used to "intercept a private communication."[151]

Further, if section 184.2 authorizations were not required to prospectively obtain text messages from recipients' devices, police would be free to conduct the very kind of long-term, open-ended, real-time communications surveillance that Part VI was designed to regulate.[152] Without judicial preauthorization on probable grounds, police would have a virtually unchecked power to covertly obtain intensely intimate information from senders, including information unrelated to the offences under investigation or any form of criminal wrongdoing.[153]

As Orin Kerr has noted, courts applying search and seizure doctrine to new technologies typically seek to restore the balance of interests that existed before that technology's emergence.[154] On this view, police should not be able to exploit technological and social changes (the advent and increasing use of electronic text communication) to conduct a type of surveillance (covert participant interceptions of communications content) historically subject to statutory and constitutional regulation.[155] It therefore makes sense to require section 184.2 authorizations for prospective acquisitions of text messages from recipients' devices. The Supreme Court has definitively held that: (1) senders maintain a reasonable expectation of privacy over messages received on recipients' devices (*Marakah*); and (2) one party's consent to prospective police surveillance of a private communication does not extinguish the other party's reasonable expectation of privacy (*Duarte*). Since section 184.2 can readily be interpreted to encompass prospective acquisition from recipients' devices (*Telus*), it should be.[156]

Interpreting section 184.2 in this manner also confers practical advantages. As many courts have noted, while first-party surveillance undoubtedly threatens communications privacy, it is not as intrusive as third-party surveillance.[157] The prerequisites for the former are accordingly less onerous than the latter. Both require issuing justices to be convinced that there are probable grounds to believe that interception will afford evidence of a specific

---

150 *Ibid*, s 183.

151 See generally *Lyons v R*, [1984] 2 SCR 633 (Part VI is "broad legislation" designed to regulate the interception of communications "reasonably expected by the originator not to be intercepted by anyone other than the intended recipient" at 664). *Contra Beairsto* Trial, *supra* note 139 at para 60.

152 See *Jones*, *supra* note 6 at paras 73–74; *Belcourt*, *supra* note 121 at paras 46–47.

153 See generally *Jones*, *ibid* at para 74; *Duarte*, *supra* note 31 at 43–44; *Wong*, *supra* note 92 at 47; *R v Araujo*, 2000 SCC 65 at para 29 [*Araujo*].

154 Orin S Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment" (2011) 125:2 Harv L Rev 476. See also *Wong*, *ibid* ("the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development" at 44); *Marakah* SCC, *supra* note 1 at para 86, Rowe J, concurring.

155 See generally *Jones*, *supra* note 6 ("[l]aw enforcement cannot receive authorization to effectively intercept future communications through the 'backdoor' of the general search and seizure regime in s. 487 of the *Code*" at para 77).

156 See generally *R v Tse*, 2012 SCC 16 at para 20 (legislation presumed to be constitutional; where a provision capable of multiple interpretations, the *Charter*-conforming option is preferred).

157 See *R v Largie*, 2010 ONCA 548 at para 24 [*Largie*], leave to appeal to SCC refused, 33982 (16 June 2011); *R v Niemi*, 2012 ONSC 5684 at paras 23–24 [*Niemi*]; *Mills* Trial, *supra* note 138 at paras 17–18.

offence.[158] But unlike first-party authorizations, third-party authorizations may only be issued by superior court justices on the application of specified government agents.[159] With some exceptions,[160] police seeking a third-party authorization must also show "investigative necessity," that is, that "other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[161] The targets of such third-party interceptions must also be notified of the surveillance, ordinarily within ninety days of the authorization's expiry.[162] Investigative necessity and notice do not apply to participant authorizations under section 184.2.[163]

In short, police may obtain participant authorizations for prospective communications on the same basis as search warrants and production orders for retrospective communications. This should not unduly burden law enforcement. If police obtain a recipient's device and lawfully search it for existing messages, they will often gain probable grounds to believe that incriminating messages will be received in the future. But if they lack such grounds, they should not be allowed to acquire future messages. Such surveillance is the very type of intrusive fishing expedition that Part VI of the *Criminal Code* and section 8 of the *Charter* were intended to forbid.

To summarize, while I argued in Part IV that people may consent to searches for text communications that they have already received, this does not authorize police to obtain incoming messages thereafter. Future text conversations are not "shared" with recipients in a manner analogous to either shared physical domains or recorded, historical text communications. Even with recipients' consent, the prospective surveillance of text communications intrudes on senders' reasonable expectation of privacy under section 8 of the *Charter* and constitutes a participant interception under section 184.2 of the *Criminal Code*. Police may only conduct such surveillance, therefore, with judicial authorization.

VI. CONCLUSION

Both the majority and dissenting reasons in *Marakah* reflected important — yet potentially conflicting — truths about the digital communications revolution. As Chief Justice McLachlin stressed for the majority, recognizing senders' expectation of privacy over text messages stored on recipients' devices will help to maintain the measure of communications privacy that citizens have come to expect in the face of technological change. But as Justice

---

158 For first-party interception, this requirement is explicit: *Criminal Code*, *supra* note 16 ("[a]n authorization may be given under this section if the judge to whom the application is made is satisfied that … there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed," s 184.2(3)(a)). For third-party interceptions, courts have interpreted the condition that the interception "be in the best interests of the administration of justice" in section 186(1)(a) to require probable grounds for evidence of a specific offence. See *Duarte*, *supra* note 31 at 45; *Araujo*, *supra* note 153 at para 20; *R v Garofoli*, [1990] 2 SCR 1421 at 1444.

159 *Criminal Code*, *ibid*, s 185(1).

160 *Ibid*, s 186(1.1).

161 *Ibid*, s 186(1)(b).

162 *Ibid*, s 196.

163 See *Largie*, *supra* note 157 at para 44 (section 8 was not violated by an absence of the investigative necessity requirement); *Niemi*, *supra* note 157 at paras 22–25 (section 8 was not violated by an absence of the notice requirement).

Moldaver noted in dissent, recognizing that expectation could make it more difficult for victims, witnesses, and police to cooperate in combatting crime.

Unfortunately, the zero-sum outlook of both camps blinded them to a positive-sum solution: permitting recipients to voluntarily consent to searches of their devices for received messages. This alternative coheres well with existing doctrine and promotes both communications privacy and law enforcement efficacy.

A recipient's consent, however, should not be sufficient to extinguish the sender's reasonable expectation of privacy over future text communications. This kind of prospective, first-party surveillance is captured by section 8 of the *Charter* and requires an authorization under section 184.2 of the *Criminal Code*. Just as participants in private, oral conversations are protected against unregulated state surveillance even if their confidants are (secretly) state agents, so should participants in private, text conversations.

[this page is intentionally blank]