McGill Law Journal
Revue de droit de McGill

"Must the Police Refuse to Look?" Resolving the Emerging Conflict in Search and Seizure Over Civilian Disclosure of Digital Evidence

Robert Diab

Volume 68, Number 4, October 2023

URI: https://id.erudit.org/iderudit/1111432ar
DOI: https://doi.org/10.26443/law.v68i4.1363

See table of contents

Publisher(s)

McGill Law Journal / Revue de droit de McGill

ISSN

0024-9041 (print)
1920-6356 (digital)

Explore this journal

Cite this article

Diab, R. (2023). "Must the Police Refuse to Look?" Resolving the Emerging Conflict in Search and Seizure Over Civilian Disclosure of Digital Evidence. *McGill Law Journal / Revue de droit de McGill*, *68*(4), 369–405. https://doi.org/10.26443/law.v68i4.1363

Article abstract

Courts in Canada are dealing more frequently with an old problem in a new guise: civilians bringing police digital evidence that engages a suspect's privacy interest (text messages, email). Do police carry out a seizure when they receive it or a search when they proceed to review it, even briefly? Should police 'refuse to look' before obtaining a warrant or other authorization? If so, why? What measure of protection would calling this a search or seizure under section 8 of the *Charter* afford Canadians? The Supreme Court of Canada has yet to decide these issues directly, and trial, appeal courts, and commentators have offered widely diverging responses to the questions they raise. In doing so, courts and commentators alike have lost sight of the Supreme Court's principled approach to what constitutes a search or seizure and when it will be reasonable. Applying this approach in *R v Marakah*, McLachlin CJ in *obiter* held that receiving a text exchange from a third party would require police to obtain a warrant before reading it, but she provided no rationale. This article articulates the Court's principled approach and shows why diverging approaches among recent courts and commentators are not compelling. More crucially, given how central digital communication has become to all of us, the article sets out a rationale for insisting on a warrant before police review texts or photos, and what is at stake in failing to provide this vital safeguard.

"Must the Police Refuse to Look?" Resolving the Emerging Conflict in Search and Seizure Over Civilian Disclosure of Digital Evidence

*Robert Diab**

Courts in Canada are dealing more frequently with an old problem in a new guise: civilians bringing police digital evidence that engages a suspect's privacy interest (text messages, email). Do police carry out a seizure when they receive it or a search when they proceed to review it, even briefly? Should police 'refuse to look' before obtaining a warrant or other authorization? If so, why? What measure of protection would calling this a search or seizure under section 8 of the *Charter* afford Canadians? The Supreme Court of Canada has yet to decide these issues directly, and trial, appeal courts, and commentators have offered widely diverging responses to the questions they raise. In doing so, courts and commentators alike have lost sight of the Supreme Court's principled approach to what constitutes a search or seizure and when it will be reasonable. Applying this approach in *R v Marakah*, McLachlin CJ in *obiter* held that receiving a text exchange from a third party would require police to obtain a warrant before reading it, but she provided no rationale. This article articulates the Court's principled approach and shows why diverging approaches among recent courts and commentators are not compelling. More crucially, given how central digital communication has become to all of us, the article sets out a rationale for insisting on a warrant before police review texts or photos, and what is at stake in failing to provide this vital safeguard.

Les tribunaux canadiens sont plus souvent confrontés à un vieux problème sous une nouvelle forme : des civils apportent à la police des preuves numériques qui mettent en jeu le droit à la vie privée d'un suspect (messages textuels, courriels). La police doit-elle procéder à une enquête lorsqu'elle reçoit ces preuves ou à une perquisition lorsqu'elle les examine, même brièvement ? La police doit-elle « refuser de regarder » avant d'obtenir un mandat ou une autre autorisation ? Dans l'affirmative, pourquoi ? Quel degré de protection les Canadiens obtiendraient-ils en qualifiant cet acte de perquisition ou de saisie en vertu de l'article 8 de la *Charte* ? La Cour suprême du Canada n'a pas encore tranché directement ces questions, et les tribunaux de première instance, les cours d'appel et les commentateurs ont apporté des réponses très divergentes aux questions qu'elles soulèvent. Ce faisant, les tribunaux et les commentateurs ont perdu de vue l'approche de principe de la Cour suprême sur ce qui constitue une fouille, une perquisition ou une saisie et sur le caractère raisonnable d'une fouille, d'une perquisition ou d'une saisie. Appliquant cette approche dans l'affaire *R v Marakah*, la juge McLachlin a estimé, en obiter, que la réception d'un échange de texte par un tiers nécessiterait que la police obtienne un mandat avant de le lire, mais elle n'a fourni aucun raisonnement. Cet article articule l'approche de principe de la Cour et montre pourquoi les approches divergentes des tribunaux récents et des commentateurs ne sont pas convaincantes. Plus important encore, étant donné que la communication numérique est devenue centrale pour chacun d'entre nous, l'article explique pourquoi il faut insister sur l'obtention d'un mandat avant que la police n'examine des textes ou des photos, et ce qui est en jeu si l'on ne fournit pas ce garde-fou vital.

* Faculty of Law, Thompson Rivers University.

Citation: (2023) 68:4 McGill LJ 369 — Référence : (2023) 68:4 RD McGill 369

Introduction

With more of our communication taking place online, courts are confronting a common scenario with greater frequency: an accused makes an admission in a text or an email to a complainant and she turns it over to police. It raises an old problem in a new guise. Do police conduct a seizure when they receive a piece of evidence from a civilian that engages a suspect's privacy? Do they carry out a search when they proceed to review the item, even briefly? Must the police refuse to look, as an appeal court has recently asked, and first obtain some form of authorization?[1] If so, why? What measure of protection would calling this a search under section 8 of the *Charter* afford Canadians?[2]

Remarkably, the Supreme Court of Canada has not yet weighed in on the core questions underlying this scenario: whether police carry out a seizure when they receive evidence from a civilian third party over which a suspect retains a privacy interest against the state, whether a cursory analysis constitutes a search, and whether police require a warrant to do so. The questions have provoked widely diverging answers among trial and appellate courts and among commentators on privacy law.[3]

In offering differing responses to third party disclosure of evidence, courts and commentators alike have lost sight of what might be called the Supreme Court of Canada's principled approach to deciding what constitutes a search or seizure and when it will be reasonable. The Court has applied this approach consistently, from its earliest cases on police receipt of evidence in *Dyment* and *Colarusso*, through a series of important cases on a reasonable expectation of privacy, including *Buhay*, *Cole*, and *Spencer*, and more recently when dealing specifically with digital evidence in *Marakah* and *Reeves*.[4] The thrust of this approach is to focus not on how police came into possession of the item — who gave what to whom and when — but to ask first whether the accused retained a reasonable privacy interest in the item against the state, and if so, whether police had authority to search or seize it. Time and again, taking this approach, the Court does not factor into its assessment of whether a search took place, or what would render the search reasonable (a warrant, consent, etc.), the status, identity, or intentions of the party providing the evidence to police.

---

1 See *R v Orlandis-Habsburgo*, 2017 ONCA 649 at para 34 [*Orlandis-Habsburgo*].

2 See *Canadian Charter of Rights and Freedoms*, s 8, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

3 The cases and commentary are discussed below.

4 See *R v Dyment*, [1988] 2 SCR 417, 55 DLR (4th) 503 [*Dyment*]; *R v Colarusso*, [1994] 1 SCR 20, 110 DLR (4th) 297 [*Colarusso*]; *R v Buhay*, 2003 SCC 30 [*Buhay*]; *R v Cole*, 2012 SCC 53 [*Cole*]; *R v Spencer*, 2014 SCC 43 [*Spencer*]; *R v Marakah*, 2017 SCC 59 [*Marakah*]; *R v Reeves*, 2018 SCC 56 [*Reeves*].

Lower courts and commentators, however, are beginning to do just this in the case of texts, emails, and screenshots: treat the matter differently on the basis that a *civilian* has brought police the item, suggesting that police receipt on voluntary disclosure is not a search or that something less than a warrant would make it reasonable.

Courts and commentators fail to follow the Supreme Court's principled approach due in part to the fact that none of the Court's cases on police receipt of evidence from third parties is directly on point. They deal with state actors transferring evidence to police, or police asking for or directly seizing evidence from a civilian third party. The closest the Supreme Court has come to addressing whether a third party *giving* police evidence engages section 8 is in *Marakah* and *Reeves*.[5] In *Reeves*, the Court held that a spouse could not consent to police seizure of a shared computer from the couple's home, on the broader principle that "[w]e are not required to accept that our friends and family can unilaterally authorize police to take things that we share."[6] This would presumably apply to a text exchange, an item in which the complainant has a shared privacy interest with an accused. In *Marakah*, the majority held that the accused retained a privacy interest in text messages found on a phone police seized from the recipient—despite the accused no longer having control of the messages.[7] In *obiter*, McLachlin CJ addressed the case of a complainant turning over a text exchange to police voluntarily. The accused might still retain a privacy interest in such messages, she suggested, even ones alleged to contain a threat against the complainant, and if so, police would need a warrant to read them; *i.e.*, that police should indeed 'just look away.'[8] What she did not explain is why. Her view is entirely consistent with the Court's principled approach, and the missing rationale for applying it here can be found in those cases.

Without a Supreme Court decision directly on point, lower courts, losing sight of the Supreme Court's principled approach to police receipt of evidence, have diverged in three directions. In some cases, the court recognizes a claimant's privacy interest in the item but holds that a third party's disclosure to police meant that police had done nothing on their part amounting to a *taking* or *interfering with* the claimant's interest.[9] In some cases, the recipient's consent authorizes police action (contrary to

---

5 See *Marakah*, *supra* note 4; *Reeves*, *supra* note 4.

6 *Reeves*, *supra* note 4 at para 44.

7 See *Marakah*, *supra* note 4 at para 55.

8 *Ibid* at para 50, discussed further below.

9 The cases are discussed in Part II below.

holdings on third party consent in *Cole* and *Reeves*).[10] A third body of cases is consistent with the Supreme Court's approach in asking, first, whether the accused retained a reasonable expectation of privacy in the messages, and where they are found to be private, holding that reading the messages without a warrant was unreasonable.

Commentators are also in dispute over how to approach police receipt of digital evidence from third parties. Steven Penney suggests that the ruling in *Cole* and *Reeves* barring one party consent over the seizure and search of a shared computer should not apply to cases involving a chat participant turning over evidence to police and that one party consent should suffice.[11] Simon Stern proposes a reasonable suspicion standard authorizing a limited search.[12] Hamish Stewart contends that whether section 8 is engaged in a third party disclosure may depend on the content of the message.[13] Each of these positions departs from the Supreme Court's principled approach in treating civilian disclosure as qualitatively different from other forms of search or seizure, calling for different standards. Yet none of these positions offers a compelling justification for departing from the Court's approach in this context.

This article aims to foreground the Court's principled approach, explain its general scope and, most crucially, articulate its rationale — its implied response to the pressing question in these cases of why police should 'just look away' when a third party brings them the printout of a chat, an email, or a photo, alleging it to contain evidence of a crime. The article also argues that McLachlin CJ's *dicta* in *Marakah* and the Court's reasoning in *Reeves* should form the basis of the Court's approach to a future case directly on point and the approach of lower courts dealing with these facts. As McLachlin CJ observed in *Marakah*, a third party's *report* of the content of a device or a private chat will "typically permit the police to obtain a warrant."[14] Why, then, insist on the officer taking that step? What extra measure of protection would this provide to potentially innocent suspects? Put another way, what mischief on the part of the state would this avoid? Drawing on the Supreme Court's earlier cases, I argue that the rationale here is that even if in most instances, police will easily

---

10 See *Cole*, *supra* note 4 at paras 78–79; *Reeves*, *supra* note 4 at para 56.

11 See Steven Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap" (2018) 56:1 Alta L Rev 1 at 9–13.

12 See Simon Stern, "Textual Privacy and Mobile Information" (2018) 55:2 Osgoode Hall LJ 398 at 435–39.

13 See Hamish Stewart, "Reasonable Expectations of Privacy as Rights" in Christopher DL Hunt & Robert Diab, eds, *The Last Frontier: Digital Privacy and the Charter* (Toronto: Thompson Reuters, 2021) at 46–47.

14 *Marakah*, *supra* note 4 at para 50.

obtain a warrant or have probable grounds for a search based on a civilian report, the requirement to establish reasonable grounds holds the state to a standard that helps to avoid casual or unnecessary intrusions into spaces or things that engage a high privacy interest. This affords all of us important assurance that the state will not be reviewing our texts, emails, or photos, on the basis of a civilian report about possible illicit content in them, unless the report is credible, the officer's belief in the probability of an offence having occurred is reasonable, and an independent third party confirms this. This has formed the standard for a reasonable search for over two centuries and, as the Supreme Court has affirmed in several closely analogous cases, nothing in the third-party disclosure scenario justifies departing from it.[15]

The article proceeds in two parts. Part I sets out the Supreme Court's principled approach by briefly canvassing decisions in a series of cases from *Dyment* to *Reeves*, to highlight the continuity and coherence of the Court's approach and to distinguish its factual underpinnings. Part II considers the emerging conflict of opinion among courts and commentators, beginning with McLachlin CJ's comments in *Marakah* on civilian disclosure of texts and recent trial and appellate decisions diverging from the principled approach. It then canvasses and critiques diverging views in recent commentary, before addressing unresolved questions about civilian disclosure to police.

The issues raised here are pressing. Civilian disclosures of text messages and screenshots are appearing in the case law more frequently. A diversity of approaches is emerging with no principled framework to unite them. Few areas involving section 8 of the *Charter* are more contested at present and, given how important digital communication is to us all, few issues in constitutional law have as wide a reach in terms of their potential impact.

I. The Supreme Court's Principled Approach

The Supreme Court's approach to whether police receipt of evidence constitutes a search or seizure under section 8 unfolds within a context of

---

15 On the pedigree of the requirement for a warrant on probable grounds, see the discussion in *Hunter et al v Southam Inc.*, [1984] 2 SCR 145 at 157–59, 11 DLR (4th) 641 [*Hunter*] of *Entick v Carrington*, (1765) 19 St Tr 1029, 1 Wils KB 275 and the Fourth Amendment to the Constitution of the United States. The Court in *Hunter* recognizes that a search can be reasonable under s 8 without a warrant; but, in ways to be explored further below, the interests to be balanced when police receive digital evidence from third parties are similar to those in other situations where the Supreme Court has insisted on a warrant or do not justify departing from the standards of reasonable search set out in *Hunter*.

other decisions that define what actions on the part of police amount to a search or seizure. These are important holdings for understanding where and why the Court has drawn boundaries around the protections in section 8. After noting these holdings briefly, I canvas the Supreme Court's principled approach by considering the cases in two groups into which they fall: those involving transfers of evidence to police from other state actors and those involving third party invitations to seize the evidence.[16]

A. When Section 8 is Engaged

Since the *Charter* applies only to state actors, the person conducting a search or seizure must be a state agent to engage section 8.[17] In *Evans*, Sopinka J held that state actors conduct a 'search' for the purposes of section 8 where "a person's reasonable expectations of privacy are somehow diminished by an investigatory technique" or where "state examinations constitute an intrusion upon some reasonable privacy interest."[18] In *Dyment*, La Forest J held that "the essence of a seizure under s. 8 is the taking of a thing from a person by a public authority without that person's consent."[19]

Police conduct a search when they inspect something;[20] when they carry out a wiretap or surreptitiously record a conversation;[21] and when

---

16 I note at the outset that the use of the phrase 'principled approach' in this paper is analogous to but different from William MacKinnon's use of it; see William MacKinnon, "*Tessling*, *Brown*, and *A.M.*: Towards a Principled Approach to Section 8" (2007) 45:1 Alta L Rev 79, where he argued for a more coherent conceptual framework to govern the finding of a reasonable expectation of privacy in cases involving sense-enhancing aids, rather than the Court's case-by-case approach. In ways to be canvassed below, this paper highlights the coherence of the approach the Court has taken in assessing a search or seizure by resort to a single framework that approaches these questions in a principled fashioned by asking not who gave what to whom, but more fundamentally: was the item private and if so, did police have authority?

17 See *RWDSU v Dolphin Delivery Ltd.,* [1986] 2 SCR 573 at 598–99, 33 DLR (4th) 174; *Vriend v Alberta*, [1998] 1 SCR 493 at paras 60, 65–66, 156 DLR (4th) 385, interpreting s 32 of the *Charter*.

18 *R v Evans*, [1996] 1 SCR 8, 131 DLR (4th) 654 at para 11.

19 *Dyment*, *supra* note 4 at 431. Not included in this often-cited definition is the requirement for a subsisting privacy interest in the item. Fish J made this explicit, writing for the majority in *Cole*, *supra* note 4 at para 34: "a taking is a seizure, where a person has a reasonable privacy interest in the object or subject matter of the state action and the information to which it gives access."

20 See *Cole*, *supra* note 4 at para 34; *R v Law*, 2002 SCC 10 at paras 26–28 (police conducting a search when they inspected documents found in a safe reported stolen).

21 See *R v Duarte*, [1990] 1 SCR 30, 65 DLR (4th) 240 [*Duarte*], La Forest J describing a wiretap as a 'search and seizure' throughout the decision.

they ask a third party for a claimant's private information.[22] Police conduct a seizure when they exercise regulatory powers to demand documents,[23] and, in the course of a regulatory inspection, when they make copies of documents.[24] The connecting thread in each of these cases is an action on the part of a state actor that involves an interference with a privacy interest the accused retains against the state.

By contrast, the Court has made various findings on what does not constitute a search or seizure, and here too the connecting thread is a lack of interference with a privacy interest. Police did not conduct a search when they merely conversed with (rather than also recording a conversation with) an informer about a target;[25] when they obtained electricity records that were already public;[26] or when they demanded a driver's license and insurance at roadside, given a lack of privacy in the information.[27] Similarly, police did not carry out a seizure when they collected garbage left at the curb, because it was abandoned.[28] A requirement in a collective bargaining agreement (of a federally regulated workplace) for the employer to provide the union periodically the names and addresses of members of a bargaining unit was not a seizure since members could reasonably expect the information would be used in this way.[29]

As the cases in the next section illustrate, when deciding whether a transfer of evidence to police or an acquisition amounted to a search or seizure, the Supreme Court focuses primarily on the question of privacy.

---

22 See *Spencer*, *supra* note 4 at paras 10–12, discussed further below.

23 See *Thomson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425 at 493–95, 67 DLR (4th) 161; *R v McKinlay Transport Ltd.*, [1990] 1 SCR 627 at 641–42, 68 DLR (4th) 568; *British Columbia Securities Commission v Branch*, [1995] 2 SCR 3 at paras 52–53, 123 DLR (4th) 462; *Canada (AG) v Chambre des notaires du Québec*, 2016 SCC 20 at para 6.

24 See *Comité paritaire de l'industrie de la chemise v Potash; Comité paritaire de l'industrie de la chemise v Sélection Milton*, [1994] 2 SCR 406 at 416, 115 DLR (4th) 702.

25 See *Duarte*, *supra* note 21 at 57; see also *R v Fliss*, 2002 SCC 16, where Arbour J held at para 12: "a conversation with an informer, or a police officer, is not a search and seizure. Only the recording of such conversation is." See also *R v Mills*, 2019 SCC 19 at para 6 [*Mills*], where an officer posing as a 14-year-old girl exchanged messages online with the accused. At para 37, Karakatsanis J and Wagner CJ took the view, endorsed by Moldaver J, that, as in *Fliss* and *Duarte*, there was no privacy in the conversation with the officer, because the officer was a direct participant in it, rather than having interfered in it. They also held that since it took place in writing, it was not a surreptitious recording or interception.

26 See *R v Plant*, [1993] 3 SCR 281 at 295–96, 145 AR 104.

27 See *R v Hufsky*, [1988] 1 SCR 621 at 638, 4 MVR (2d) 170.

28 See *R v Patrick*, 2009 SCC 17 at para 73.

29 See *Bernard v Canada (AG)*, 2014 SCC 13 at paras 32–33, 41–42.

The Court's readiness to draw the inference that asking, glancing, taking, or receiving can amount to a search or seizure suggests that the standard is low—an interference with a privacy interest to *any* degree suffices to meet the test. In ways to be seen, this forms an important part of the Court's principled approach and becomes especially contentious in the case law and commentary on civilian disclosure.

B. State Actors Giving Police an Item

The Supreme Court laid the foundation for its approach to police receipt of evidence from a third party in *Dyment* and *Colarusso*.[30] It then applied the approach in a series of cases (considered below), but this section canvasses *Dyment*, *Colarusso*, and *Cole* to show that a state actor coming into possession of evidence for one purpose can give rise to a search or seizure under section 8 by turning it over to police without being asked. The turnover in these cases is relevant to civilian disclosure to police in three ways. The Court in each case holds that the transfer of an item to police amounted to a search or seizure not because a state agent initially obtained the evidence or gave the item to police, but rather, because the accused retained a privacy interest against law enforcement *when the officer received it*. The cases also hold that police conduct a seizure when police merely receive the item or a search when they proceed to analyze or make investigative use of it—despite *knowing or suspecting* what it contains. And finally, the Court holds that the search or seizure required a warrant on probable grounds to be reasonable. The standard for a reasonable search turns not on *how* police obtained the item but on *what* they obtained.

In *Dyment*, a doctor took a vial of blood from an accused for medical purposes, after a car accident and without his knowledge. Discovering the accused had been drinking, the doctor decided to turn over the sample to police.[31] In concurring opinions, the majority held that the officer's receipt of the samples constituted a 'seizure,' for the reasons La Forest J set out. Whether the officer's receipt of the sample amounted to a seizure did not turn, for La Forest J, on whether the doctor volunteered or the officer asked for the sample. Evidence of the conversation between the two was unclear.[32] The matter turned on whether a privacy interest persisted. "If I were to draw the line between a seizure and a mere finding of evidence," La Forest J wrote, "I would draw it logically and purposefully at the point

---

30 See *Dyment*, *supra* note 4; *Colarusso, supra* note 4.

31 See *Dyment*, *supra* note 4 at 422.

32 *Ibid* at 434.

at which it can reasonably be said that the individual had ceased to have a privacy interest in the subject-matter allegedly seized."[33]

The officer's receipt of the sample became a seizure in *Dyment* not because the doctor chose to make a different use of it, but because the accused retained a privacy interest in the sample when the officer received it.[34] A further element assumed in La Forest J's discussion but not made overt was the officer's intention to use the sample for an investigative purpose.[35] Given the high privacy interest in the body, a seizure without a warrant was unreasonable.[36] McIntyre J, in dissent, declined to construe the officer's receipt of the sample as a seizure, employing an approach that has reappeared in recent case law (canvassed in Part II, below). Any breach of privacy here was due to the doctor and impliedly—McIntyre J is silent on this point—the privacy interest ended there.[37] The officer was under a duty to make use of 'real evidence' and there was nothing improper in his doing so.[38]

In *Colarusso*, police took the accused to hospital following a motor vehicle accident involving a fatality in which alcohol was suspected.[39] The accused consented to staff taking a blood sample and, with an officer's assistance, a urine sample "for medical purposes."[40] Pursuant to powers in the *Coroners Act*, the coroner obtained the samples from a lab technician and turned them over to a police officer at the hospital for storage at a forensic lab for later analysis.[41] The Crown called a forensic toxicologist who had analyzed the samples at the lab at the coroner's request, to assist in the latter's investigation under the Act. The toxicologist's blood-alcohol readings from the samples formed a basis for the accused's conviction. In a 5-4 decision, a majority of the Supreme Court affirmed the trial judge's finding that when the officer assisted in obtaining the urine sample, he

---

33 *Ibid* at 435.

34 *Ibid* at 434. As Laforest J puts it, "the sample was surrounded by an aura of privacy meriting *Charter* protection;" *ibid* at 435.

35 *Ibid* at 431–32; this assumption runs through the discussion (*i.e.*, in discovering alcohol in the sample, the doctor gave it to the officer as potential evidence of an offence, and the officer accepted it to potentially use for that purpose).

36 *Ibid* at 438; *ibid* at 422 where LaForest J notes the incident predates the inclusion in the *Criminal Code*, RSC 1970, c C-34, s 238(3) of a power to demand a blood sample on probable grounds to believe the accused has driven while impaired.

37 *Ibid* at 442: "If there was a wrongful seizure, it was made by the doctor and there is no evidence which would implicate the police officer."

38 *Ibid*.

39 See *Colarusso*, *supra* note 4 at 30.

40 *Ibid* at 30.

41 *Ibid* at 30–32, discussing the *Coroners Act*, RSO 1980, c 93, s 16(2)(c), 16(5).

was not conducting a seizure, but merely assisting hospital staff. However, after the coroner had arrived, because the accused retained a privacy interest in the sample, what followed amounted to an unreasonable seizure in two ways. The officer carried out a seizure when he *received* the samples from the coroner for storage at a forensic lab because they were then available for a prosecutorial purpose, the officer intended "from the outset" to use them for that purpose, and did so without a warrant.[42] Alternatively, the coroner's seizure from hospital staff became unreasonable by making the samples available to police and failing to confine his use of them to the (non-criminal) purposes set out in the *Coroners Act*.[43]

The minority in *Colarusso* held that the coroner's initial seizure from hospital staff was the only authority the Crown needed to make lawful use of the sample for the purpose of prosecution. Police delivering the samples to the lab did not amount to a seizure, since they were "essentially acting as a courier."[44] There was no *taking* by police. The coroner's involvement of police as a courier, the officer's storage of the samples at the lab, and the toxicologist's analysis were all authorized under the *Coroners Act* and fell within the scope of the coroner's inquiry. The fact that the inquiry happened to produce evidence relevant to the criminal case is unfortunate for the accused but did not make any part of it a prosecutorial seizure.[45] Dissenting judges saw "no difference, as far as the police actions are concerned, between this case and one in which the Crown subpoenas a hospital lab technician to give evidence that came into existence during *bona fide* medical procedures and is relevant to a criminal proceeding."[46]

The dispute between the majority and minority in *Colarusso* is framed as one turning on the limits of the accused's consent. It might be framed another way: the accused's consent was not fully informed. Had he known that taking a sample 'for medical purposes' might include some use by the coroner, he might not have consented. The larger point, however, is that both the majority and minority agree on the central issue: was the blood sample private? Did the accused's initial consent permit the state to do what it did here? The two sides disagree on the answer, but they agree that whether there was a seizure under section 8 turns not on who gave

---

42 *Ibid* at 58–59. At 60, La Forest J also describes police as having independently seized the samples: "Given the effective control by the police over the samples held by another agent of the state, I would conclude that the police seized the blood sample from the appellant independently of the coroner's seizure (although the police seizure was obviously facilitated by the actions of the coroner)." (*ibid*).

43 *Ibid* at 58, 62–65.

44 *Ibid* at 42.

45 *Ibid* at 42–44.

46 *Ibid* at 42.

what to whom, but on the validity and scope of the initial consent—which is another way of asking: did he retain some measure of privacy in the sample?[47]

In *Cole*, a technician in a high school discovered nude pictures of a student on a teacher's board-issued laptop and reported them to the principal, who gave the laptop to police.[48] Without obtaining a warrant, police examined the content of the device and made a mirror image of its hard drive. Cole was charged with possession of child pornography. The Supreme Court held that in taking custody of the laptop for more than a brief period (to obtain a warrant) and examining its contents without a warrant, police had carried out an unreasonable search and seizure.[49] In the Court's view, Cole retained a privacy interest in the content of the laptop given to police due in part to the understanding that he could make some personal use of it.[50] School officials may have been authorized to seize the device under a statutory duty to "maintain a safe school environment", but this did not provide *police* authority to seize or search for a criminal investigative purpose.[51]

Relevant to the present discussion is how Fish J describes the handover and initial conduct of police upon receipt of the items. He makes clear that school officials were "entitled to inform" police of the illicit content on the device and police might have used this information to obtain a warrant.[52] But "receipt of the computer from the school board did not afford the police *warrantless access* to the personal information contained within it. This information remained subject, at all relevant times, to Mr. Cole's reasonable and *subsisting* expectation of privacy."[53] This raised the ques-

---

47 A contrast can be drawn here with the facts in *Quebec (AG) v Laroche*, 2002 SCC 72, which LeBel J, for the majority, distinguished from those in *Colarusso* in holding, at paras 82–84, that when regulators turned over to police evidence obtained when the owner of a garage disclosed information required under a regulatory scheme intended to oversee the sale and repair of vehicles, they did not carry out a seizure since the owner did not have a reasonable expectation of privacy in the information disclosed to regulators—no privacy in relation to the state in general. The implication here was that it would not have been reasonable to assume that irregularities involving criminal activity would not be shared with police.

48 See *Cole*, *supra* note 4 at paras 4–5.

49 *Ibid* at paras 66–79. In separate reasons, Abella J agreed with the majority on section 8, but contrary to the majority would have excluded the evidence under section 24(2). See *ibid* at paras 134–35.

50 *Ibid* at paras 66–79.

51 *Ibid* at paras 62, 65.

52 *Ibid* at para 73.

53 *Ibid.*

tion of whether merely taking custody of the laptop constituted a seizure under section 8. Focusing on the receipt itself, Fish J writes:

> The police may well have been authorized to take physical control of the laptop and CD *temporarily, and for the limited purpose of safeguarding potential evidence of a crime until a search warrant could be obtained*. However, that is not what occurred here. Quite the contrary: The police seized the laptop and CD *in order to search their contents for evidence of a crime* without the consent of Mr. Cole, and without prior judicial authorization.[54] [Emphasis in the original]

The need to posit temporary authority to hold the computer "until a search warrant could be obtained" implies that merely receiving the device constituted a seizure under section 8. This was premised on the finding that Cole had a "reasonable and *subsisting* expectation of privacy", along with the officer's investigative purpose in taking custody of the item. It did not turn on *the identity* of the party bringing police the item.

The Crown had also argued that police could rely on the school board's consent to search the laptop, since the board owned it. The "underlying premise of this submission" Fish J held was that "a third party may waive another person's privacy interest — thereby disengaging that person's guarantee under s. 8 of the *Charter*."[55] Rejecting this claim, the Court drew a bright line: a third-party may not waive another person's privacy interest.[56] The rationale is directly relevant to civilian disclosure of digital evidence. As Fish J notes, the American version of the third party consent doctrine is premised on a risk that a party to whom a person makes a disclosure may turn it over to police.[57] The Supreme Court rejected the risk analysis in *Duarte* and *Wong*.[58] Moreover, Fish J held, third party consent fails to satisfy Canadian law on valid consent, which requires that it be "both voluntary and informed."[59] Third party consent would entail police interference with a person's privacy "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."[60]

---

54 *Ibid* at para 65.

55 *Ibid* at para 74.

56 *Ibid* at paras 74–79.

57 *Ibid* at paras 75–76, Fish J citing *United States v Matlock*, 415 US 164 (1974), *Illinois v Rodriguez*, 497 US 177 (1990), and *United States v Ziegler*, 474 F (3d) 1184 at 1191 (9th Cir 2007).

58 See *Cole*, *supra* note 4 at para 76, citing *Duarte*, *supra* note 21 at 47–48 and *R v Wong*, [1990] 3 SCR 36 at 45, 11 WCB (2d) 350 [*Wong*].

59 *Cole*, *supra* note 4 at para 78.

60 *Ibid*.

C. Police Asking for or Taking an Item from a Third Party

The Supreme Court has also applied its principled approach in a series of cases where police ask a third party for information or a civilian reports a crime and invites police to seize the evidence. As it had done in *Dyment*, *Colarusso*, and *Cole*, the Court finds a search or seizure and decides whether it was reasonable not by focusing on details surrounding the taking or receiving of the item but, rather, on the *principled* basis of asking, first, whether police actions involved an interference with a persisting privacy interest and, if so, whether police had authority.

Buhay offers the clearest example of the Court's principled approach, by drawing out its logic most explicitly. The accused rented a locker in a bus depot and security guards detected an odor of marijuana emanating from it.[61] An agent for Greyhound opened the locker and guards found a duffle bag inside containing marijuana. The guards placed it back, locked the locker, and called police. They directed police to the locker; officers smelled marijuana emanating from it; a Greyhound agent opened the locker, and an officer seized the bag. Arbour J, for a unanimous Court, affirmed the findings of the courts below that in their initial search, guards were not state agents, having acted independently from police.[62] But when a guard opened the locker and the officer took the bag, police conducted a seizure under section 8. Encapsulating holding, Arbour J wrote:

> In this case, it cannot reasonably be said that the appellant had ceased to have a privacy interest in the contents of his locker. The subsequent conduct of the police should be considered a seizure within the meaning of s. 8. I see no basis for holding that a person's reasonable expectation of privacy as to the contents of a rented and locked bus depot locker is destroyed merely because a private individual (such as a security guard) invades that privacy by investigating the contents of the locker. The intervention of the security guards does not relieve the police from the *Hunter* requirement of prior judicial authorization before seizing contraband uncovered by security guards. To conclude otherwise would amount to a "circumvention of the warrant requirement".[63]

Despite a third-party directly leading police to the locker and police knowing its contents, the accused had retained a privacy interest against the state. Once again, the assessment turned not on the identity of the actors, their knowledge, or the choreography of their encounter, but on the question of a subsisting privacy interest.

---

61 See *Buhay*, *supra* note 4 at para 3.

62 *Ibid* at paras 30–31.

63 *Ibid* at para 34.

In *Spencer*, the Court held that when police asked a third party for information pertaining to the accused, police carried out a search because the accused had a privacy interest in the information. Police had asked Shaw for the subscriber information attached to an internet protocol address implicated in a child pornography offence.[64] The Court held that a person retains a privacy interest in this information against the police, despite the allowance for voluntary disclosure of it in the *Personal Information Protection and Electronic Documents Act*.[65] Cromwell J, for the Court, framed the entire decision around the assertion that whether Spencer's rights under section 8 were engaged depended on whether he had a privacy expectation in the information at issue. "If he did," Cromwell J asserted without elaboration, "then obtaining that information was a search."[66] Since police had no authority for requesting the private information at issue, their request, receipt, and use of it violated section 8. The Court did not decide what would authorize a reasonable search here, aside from "exigent circumstances or a reasonable law".[67] Yet the need for authority, where a service provider *volunteers* the information, demonstrates yet again that whether police conduct a search and when it would be reasonable does not turn on the fact of voluntarily disclosure.

In *Marakah*, police investigating firearms offences obtained text messages authored by the accused when they searched the recipient's phone without authority.[68] The majority of the Court held that a sender can, in some cases, retain a reasonable privacy interest in messages they send despite not having control over them in the recipient's hands. The decision turned on two core ideas: the high degree of privacy accorded to text messages,[69] and the Court's rejection of the risk analysis in *Duarte*.[70] McLachlin CJ held that "[t]o accept the risk that a co-conversationalist could disclose an electronic conversation is not to accept the risk of a dif-

---

64 See *Spencer*, *supra* note 4 at paras 10–12.

65 See *Spencer*, *supra* note 4 at para 73, finding that neither the *Criminal Code*, RSC 1985, c C-46, s 487.014(1) [*Criminal Code*] (at the time) nor the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 7(3)(c.1)(ii) create a "power to conduct a search for subscriber information."

66 *Spencer*, *supra* note 4 at paras 16, 67, where he also notes: "[w]here a police officer requests disclosure of information relating to a suspect from a third party, whether there is a search depends on whether, in light of the totality of the circumstances, the suspect has a reasonable expectation of privacy in that information."

67 *Ibid* at para 73.

68 See *Marakah*, *supra* note 4 at para 2.

69 See *ibid* at paras 35, 37, noting: "it is difficult to think of a type of conversation or communication that is capable of promising more privacy than text messaging"; they are "capable of revealing a great deal of personal information."

70 See *Duarte*, *supra* note 21 at 39–42, 47–48.

ferent order that the state will intrude upon an electronic conversation absent such disclosure."[71] A sender does not have full control over a message they have sent, but they do exercise "meaningful control over the information they send by text message by making choices about how, when, and to whom they disclose the information."[72] For Moldaver and Côté JJ in dissent, a sender's "total absence of control" over a message in a recipient's hands renders any expectation of privacy on the part of a sender unreasonable.[73]

For both the majority and the dissent in *Marakah*, whether police carried out a search or seizure against the accused in obtaining his texts from a recipient's phone turned—as it has in all of the Court's earlier cases on police acquisition of evidence—on whether he retained a privacy interest in the item at issue. Finding that he did retain an interest, the majority assumed, without discussion, that nothing about the acquisition of the texts from the recipient's phone called for a lower standard for searching it. They held it to be unreasonable without a warrant or other authority.[74]

The Supreme Court took a similar approach of looking first at the question of privacy in *Reeves*, a case involving police taking an item with a civilian third-party's consent.[75] Reeves' spouse told police she found child pornography on a home computer she shared with her spouse. An officer came to the home and, with her consent, took the computer and held it for four months without a warrant and without reporting the seizure (as is required under section 489.1 of the *Criminal Code*). All members of the Court agreed that the spouse's consent did not serve to waive Reeves' privacy interest in the computer against law enforcement, and that police removal of it constituted an unreasonable seizure.[76] The holding turns on the majority's affirmation of three propositions: from *Marakah*, the notion that shared control over an item is not fatal to the finding that Reeves re-

---

71 *Marakah*, *supra* note 4 at para 40, citing *Duarte*, *supra* note 21 at 44.

72 *Marakah*, *supra* note 4 at para 39. A possible limit to this control would be choosing to have a conversation with a person who turns out to be an undercover officer, as was the case in *Duarte*, *supra* note 21, *Fliss*, *supra* note 25, and *Mills*, *supra* note 25. But in that scenario, police would not be *intruding* on a conversation assumed to be private, they would be partaking in it directly. Nothing said to an officer here would be private, but the surreptitious recording of it would engage a privacy interest and constitute a search.

73 *Marakah*, *supra* note 4 at para 133.

74 *Ibid* at paras 56–57, 65, holding that police should have obtained a warrant.

75 See *Reeves*, *supra* note 4 at para 1.

76 *Ibid* at paras 27–58.

tained a privacy interest;[77] the point from *Cole* that a co-possessor of a privacy interest cannot waive the accused's privacy interest, because the risk of third party disclosure does not vitiate the need for first party consent;[78] and that the heightened privacy interest that computers attract calls for heightened protections—either a warrant or valid consent from each privacy holder.[79] The majority's reasoning on the second of these propositions speaks directly to the problem of third party disclosure of digital evidence to police.

The Crown sought to distinguish *Cole* by arguing that "Reeves' spouse had an equal and overlapping privacy interest in the computer."[80] Whereas in *Cole*, the school board owned the computer but Cole was its only user, here there were two users. Karakatsanis J, on behalf of the majority in *Reeves*, held "I cannot accept that, by choosing to share our computers with friends and family, we are required to give up our *Charter* protection from state interference in our private lives. We are not required to accept that our friends and family can unilaterally authorize police to take things that we share."[81] The Crown raised the concern that this reasoning would "prevent victims of crime who have received threatening or harassing text messages from showing them to the police."[82] Karakatsanis J declined to address the issue, noting it was not the question before the Court.[83] Yet, given the holding in this case that police need each party's consent to seize a shared computer, it would make sense to take a different approach to texts only if they entailed a different *kind* of shared interest. A holding to this effect, however, would run contrary to the Court's approach to text messages in *Marakah* as capable of retaining privacy without control.

Reeves is also instructive on a further point: whether mere receipt of digital evidence would be a seizure. Karakatsanis J suggests that it would be a seizure by virtue of its consequences:

> ...while the privacy interests engaged by a seizure may be different from those engaged by a search, Reeves' informational privacy interests in the computer data were still implicated by the seizure of the computer. When police seize a computer, they not only deprive individuals of *control* over intimate data in which they have a rea-

---

77 *Ibid* at paras 37–39.

78 *Ibid* at paras 48–52.

79 *Ibid* at paras 34–35.

80 *Ibid* at para 40.

81 *Ibid* at para 44.

82 *Ibid* at para 46.

83 *Ibid*.

> sonable expectation of privacy, they also ensure that such data remains *preserved* and thus subject to potential future state inspection.[84]

If the mere taking of a computer is held to be a seizure in this passage by depriving a person of a different order of control entailed in sharing with a friend (state preservation, future inspection)—the same should apply to all forms of digital evidence, including texts or emails.

This survey of Supreme Court holdings was meant to show the consistency and coherence of the Court's approach to deciding whether a search or seizure has taken place under section 8 and whether it is reasonable. Amidst a variety of circumstances touching on police intentions, degrees of knowledge, and particulars around the physical handling of the evidence, the Court has continuously applied a *principled* approach, asking *not* 'who gave what to whom?' but rather, 'did the accused retain a reasonable privacy interest in the item police acquired?' In every case where the answer is yes, the Court holds there was a search or seizure. The Court also assesses the appropriate standard for whether it was reasonable (*i.e.*, did it require a warrant, only probable grounds, first party consent, etc.) strictly in relation to the ideas of (a) a state intrusion into (b) a reasonable privacy interest. In none of these cases does the third party's identity or intentions matter to whether police engaged section 8 or *justify a lesser standard* for a search than would otherwise apply. So long as in asking for, taking, or receiving the item, police had an investigative purpose (*Dyment*, *Colarusso*, *Cole*) or took investigative action (*Buhay*, *Marakah*, *Reeves*) and a privacy interest persisted, the search or seizure required a warrant on probable grounds.[85]

II. Conflicting Views on Third Party Disclosure of Digital Evidence

In the cases above, a state actor gives police evidence or police request it from a third party. The Court has yet to decide a case where a civilian volunteers an item to police, leaving open two questions. Does an officer conduct a seizure merely by receiving the item or a search by perusing it, even briefly?

---

[84] *Ibid* at para 30.

[85] See *Spencer*, *supra* note 4, as an exception in that the Court abstained from deciding what would constitute a reasonable search law for obtaining subscriber information. Notably, however, the Court avoided any suggestion that the usual presumption would not apply in that case: *i.e.*, that a warrantless search would be presumptively unreasonable. In the wake of *Spencer*, Parliament has not amended the *Criminal Code* to provide a special warrant for subscriber ID. Police use the 'Production Order' warrant power for this in *Criminal Code*, s 487.01, which requires reasonable and probable grounds.

The closest the Supreme Court has come to addressing these questions is in *obiter* in *Marakah*.[86] The *obiter* is directly on point in dealing with digital evidence—civilian disclosure of text messages. In ways to be seen in what follows, McLachlin CJ's position is consistent with the Court's principled approach to search and seizure, but it runs contrary to lower court holdings and recent commentary. I look first at the *obiter* in *Marakah* and draw on the Court's earlier holdings to trace out the rationale supporting it, before contrasting it with conflicting case law and commentary.

A. McLachlin CJ's Obiter *in* Marakah

In *Marakah*, as noted, the majority held that a recipient can retain a privacy interest in a text message police obtain from a recipient's device.[87] For Moldaver and Côté JJ in dissent, this raised a host of practical concerns for police and courts.[88] The Chief Justice makes her comments on third party disclosure in response to these concerns.

Notably, Moldaver J, who authored the dissenting opinion, recognized that if the Court finds that a sender can retain a reasonable privacy interest in messages found on a recipient's phone, police receipt of them on voluntary disclosure by the recipient *would entail a search or seizure*.[89] Given the Court's dismissal of third party consent in *Cole*, "the police would never be able to obtain information about an accused through electronic communications offered by victims and witnesses on consent."[90] As a consequence, the "overall number of instances where the police will be required to obtain judicial authorizations to gather evidence could increase dramatically."[91] The increase in warrant applications would slow investigations, prolong trials, and "strain police and judicial resources" in a justice system "stressed to the breaking point."[92] Most concerning still: "police may require a warrant even where a victim or his or her parents

---

86 See *Marakah*, *supra* note 4.

87 *Ibid* at paras 55–57, 65.

88 *Ibid* at paras 177–88.

89 See *ibid* at para 181: "Under the Chief Justice's approach, where police search a cellphone or other device for an electronic communication, any participant to that communication would have standing to challenge the lawfulness of the search. The same may be true even where a witness voluntarily shares an electronic communication with the police […] As such, in these circumstances, s. 8 may be engaged and a search warrant may well be necessary to comply with s. 8."

90 *Ibid* at para 182.

91 *Ibid*.

92 *Ibid* at paras 185, 187.

voluntarily provide police with threatening or offensive text messages"—a fact the majority conceded.[93]

McLachlin CJ offered two arguments in response, the first going to the heart of the Court's framework for reasonable search in section 8:

> Moldaver J. rejects any interpretation of s. 8 that would allow sexual predators or abusive partners to retain a reasonable expectation of privacy in text messages that they may send to their victims (para. 169). However, since *Hunter*, prior judicial authorization has been relied on to preserve our privacy rights under s. 8. In consequence, the fruits of a search cannot be used to justify an unreasonable privacy violation. To be meaningful, the s. 8 analysis must be content neutral.[94]

McLachlin CJ might also have added here that whether one has a reasonable expectation of privacy in something is a normative question and does not turn on whether the use one makes of a space or a thing is criminal in nature.[95] Her second argument is that the majority's position might make police work more onerous, but there is "nothing in the record to suggest that the justice system cannot adapt to the challenges", nor is it the case that "text messages sent by sexual predators to children or sent by abusive partners to their spouses will not be allowed into evidence."[96] Where obtained in violation of section 8, messages might still be admitted under section 24(2) of the *Charter*.[97]

The Chief Justice then ventured an opinion on how the holding in *Marakah* would apply to a civilian who brings police evidence:

> Assuming that s. 8 is engaged when police access text messages volunteered by a third party [...], a breach can be avoided if the police obtain a warrant prior to accessing the text messages. As stated in *Cole*, "[t]he school board was . . . legally entitled to inform the police of its discovery of contraband on the laptop" and "[t]his would doubtless have permitted the police to obtain a warrant to search the

---

93 *Ibid* at para 181.

94 *Ibid* at para 48, referring to *Hunter*, *supra* note 15.

95 See *Wong*, *supra* note 58 at 45–46, LaForest J holding for the majority: "the problem of determining whether a person had a reasonable expectation of privacy in given circumstances" depends on whether, "by the standards of privacy that persons can expect to enjoy in a free and democratic society, the agents of the state were bound to conform to the requirements of the *Charter* when effecting the intrusion in question." The Court in that case found the accused had a reasonable privacy interest against the state in a hotel room in which he had run an illegal gaming operation. See also *R v Tessling*, 2004 SCC 67 at para 42: "[e]xpectation of privacy is a normative rather than a descriptive standard."

96 *Marakah*, *supra* note 4 at paras 49, 53.

97 *Ibid* at para 52.

> computer for the contraband" (para. 73). Similarly, victims of cyber abuse are legally entitled to inform the police, which will typically permit the police to obtain a warrant. The police officers will be aware that *they should not look at the text messages in question prior to obtaining a warrant*.[98] [emphasis added]

An officer would need a warrant to look at the messages because even looking would constitute a search. In keeping with the Court's principled approach, receiving a copy of the message from a victim, rather than police asking for or taking it, *does not change the analysis*. It turns on whether the accused retained a privacy interest in the message. Nor does the situation call for a different standard. Put another way, for Moldaver and Côté JJ, what would make for a reasonable search turns on *how* police obtained the item (*i.e.*, the fact of receiving the item from a civilian). For McLachlin CJ, what would make for a reasonable search turns on *what* police obtained.

The Chief Justice explained why, in her view, the dissent's concerns do not pose a significant impediment to recognizing this as a search or seizure and insisting on a warrant. But she did not explain why police should require a warrant or other authority. In other words, insisting that police should obtain a warrant may be consistent with the view from *Hunter* onward that the "fruits of a search cannot be used to justify an unreasonable privacy violation" and the privacy analysis being content neutral. But she does not explain why, in *the specific case* of a police officer meeting with a civilian, the officer must avoid looking at a printed copy of a chat she had with a potential suspect without first obtaining a warrant (or having other authority). If, as McLachlin CJ pointed out, a civilian's report will "typically permit the police to obtain a warrant", why insist on the officer taking that step? What extra measure of protection does this provide to potentially innocent suspects? What mischief on the part of the state does it avoid?

The Court has confronted this issue in various cases where obtaining a warrant may seem like a formality. For example, in *Duarte*, the Court held that even where police have one party's consent to conduct a wiretap (*i.e.*, an informant), they still need to obtain a warrant.[99] In *Spencer*, police needed authority to carry out a search before asking Shaw for a user's subscriber information, despite the fact that privacy law permits a service

---

[98] *Ibid* at para 50. The Chief Justice opines on this scenario as one of three possibilities in paras 50–52 as to how text message a third party gives police may be admitted: the party describes their content and police obtain a warrant before reading them; police proceed to read them without a warrant but rely on other authority or the texts are found not to attract a reasonable expectation of privacy; and police read them in violation of section 8 but they are admitted under section 24(2) of the *Charter*.

[99] See *Duarte*, *supra* note 21 at 57.

provider to make disclosures to law enforcement.[100] The Court in these case offers two main reasons for insisting on a warrant even if, in most instances, police will easily obtain one or have grounds for a search. The requirement to establish grounds holds the state to a certain standard that helps to avoid casual or unnecessary intrusions into our privacy. And the hurdle or hindrance is worth the trouble it imposes upon police because the privacy interest in the item or space they would search or seize is high and the hurdle makes unnecessary intrusions less likely.

The Court in *Reeves* applies this reasoning explicitly in relation to police seizure of a computer. As Karakatsanis J writes:

> The unique and heightened privacy interests in personal computer data clearly warrant strong protection, such that specific, prior judicial authorization is presumptively required to seize a personal computer from a home. This presumptive rule fosters respect for the underlying purpose of s. 8 of the *Charter* by encouraging the police to seek lawful authority, more accurately accords with the expectations of privacy Canadians attach to their use of personal home computers and encourages more predictable policing.[101]

As noted above, the Court in *Marakah* accorded a similar high degree of privacy to text messages ("it is difficult to think of a type of conversation or communication that is capable of promising more privacy than text messaging").[102] If both computers and texts engage a high degree of privacy, the Court's insistence on a warrant or other authority for a search or seizure where police lack the accused's consent is meant not simply to burden police, but to better protect privacy through more predictable policing. As the Court held in *Hunter*, predictable policing and protecting privacy are both supported in turn by clear rules and objective standards that help to avoid unreasonable searches before they occur.[103]

The unspoken rationale for applying these principles to the case of an officer about to scan even only a page-long print out of a text exchange a

---

[100] See *Spencer*, *supra* note 4 at paras 73–74.

[101] *Reeves*, *supra* note 4 at para 35.

[102] *Marakah*, *supra* note 4 at para 35.

[103] See *Hunter*, *supra* note 15 at 167, Dickson J, as he then was, noted: "The purpose of an objective criterion for granting prior authorization to conduct a search or seizure is to provide a consistent standard for identifying the point at which the interests of the state in such intrusions come to prevail over the interests of the individual in resisting them." At 160, Dickson J held that the purpose of s 8 is "to protect individuals from unjustified state intrusions upon their privacy. That purpose requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in my view, can only be accomplished by a system of prior authorization, not one of subsequent validation." (Emphasis in the original.)

civilian has brought them is that it affords everyone an important measure of assurance. We need not be concerned that the state may be reading our texts or email on the basis of a civilian report about possible illicit content in them, unless the report is credible, the officer's belief in the probability of an offence having occurred is reasonable, and an independent third party confirms this. Insisting upon these requirements is consistent with a wider societal expectation that our conversations, photos, or emails will not easily end up in the hands of the state—for preservation or investigation. Conversely, given the ease with which digital evidence can be shared, stored, or turned over, the failure to provide this safeguard imperils everyone's sense of privacy, dignity, and autonomy.[104]

When would police not have reasonable grounds for a warrant, resulting in unnecessary intrusions on private messages or emails? In a few cases. One would be upon initial or early contact with a complainant, when the complainant has not yet finished conveying the information they have to convey about the allegations and the content of the document at issue. One can readily imagine a scenario in which a complainant provides an officer a document early in the course of a meeting to give a statement and the officer perusing it before obtaining all the facts. Another scenario would be when what a complainant tells police about the content of an exchange, photo, or email does not give rise to a reasonable probability that the document at issue will contain evidence of an offence (as is required under section 487 of the *Criminal Code*). For example, a person might allege that they have been assaulted but only vaguely describe the content of an exchange or email in a manner that leaves unclear whether the document is likely to contain evidence relevant to the assault. Further scenarios where police might lack grounds would include a complainant making an allegation that does not amount to an offence (*i.e.*, the suspect did something offensive or obnoxious, but not illegal) or frailties in the complainant's account cast into doubt the *likelihood* than offence has been committed and evidence of it is to be found in the document to be searched. Requiring the officer to hold off on looking at the evidence until gathering all the facts—and obtaining independent confirmation of their assessment—would avoid unnecessary intrusions into private emails or exchanges in each of these cases.

---

[104] See Stern, *supra* note 12 at 402, noting "[t]he interests that animate privacy rights generally in this area—the autonomy, integrity, and dignity interests of individuals in a free and democratic society—would be radically eroded if people had to assume that whenever they communicate with others, the content is presumptively open to random search by the police, unsupported by any articulable justification, whenever the content is preserved in a form that persists after the communication has been received." Stern cites *Hunter*, *supra* note 15 at 159 and *R v Plant*, *supra* note 26 at 293 as sources tying privacy to these interests.

B. Conflicting Approaches Among Lower Courts

In the absence of a Supreme Court decision directly on point, uncertainty remains. Yet the scenario of a suspect making inculpatory admissions in an email or text to a complainant who turns it over to police is becoming all too common. Trial and appeal courts have arrived at different conclusions about whether police seized or searched an item on receipt or review of it, many of them by neglecting to apply the Supreme Court's principled approach.

The reasoning in recent cases takes one of three forms. In some cases, the court recognizes a claimant's privacy interest in the item but holds that a third-party's voluntary disclosure of it to police (or a screenshot of it) meant that police had done nothing on their part amounting to a *taking* or *interfering with* the claimant's interest.[105] In some cases, the recipient's consent authorizes police action.[106] A third body of cases is consistent with the Supreme Court's principled approach, in taking the primary question to be whether the accused retained a reasonable expectation of privacy in the messages at issue or what is depicted in a screenshot or found on a device.[107] A brief look at some of these cases shows how peculiarities in the evidence, or how police obtain it, can lead judges to overlook an underlying simplicity in the issues.

In *King*, the accused's wife, suspecting him of infidelity, obtained his password, accessed his devices, and discovered what she believed was child pornography.[108] She took screenshots of some of the images on his devices and saved the screenshots to a USB drive. She described to police the images she saw and gave the USB drive to the officer. He in turn examined the screenshots on the disk and used the information to obtain a warrant to seize and search King's devices. The trial judge held the accused had a privacy interest in the screenshots the officer reviewed on the USB drive since the subject matter of the search was not the drive or the screenshots themselves, but, in effect, the glimpse they afforded inside

---

[105] See *R v King*, 2021 ABCA 271 at paras 14–15 [*King* ABCA]; *Estrella Llaneza c R*, 2019 QCCQ 3012 at paras 39, 42, where the court held the sender had no privacy in the sent messages turned over, but also held at para 29 that having been given the phone by the recipient, extracting the messages and reading them, "police did not take anything from the accused." See also *R v Admurski #4*, 2022 ONSC 1338 at para 43 [*Admurski*]; *R v AK*, 2022 ABQB 503 at paras 37–40 [*AK*], discussed further below.

[106] See *Orlandis-Habsburgo*, *supra* note 1 at paras 33–34; *R v Lowrey*, 2016 ABPC 131 at paras 83–85 [*Lowrey*]; *R v Phagura*, 2019 BCSC 1638 at paras 58–62 [*Phagura*] – all discussed further below.

[107] Among other cases discussed below are *R v King*, 2019 ABPC 236 [*King* ABPC] and *R v Morgan*, [2020] OJ No 2330 (Ont Ct J) [*Morgan*].

[108] See *King* ABPC, *supra* note 107 at para 7.

King's devices. Looking at the screenshots, the officer could see "how [the accused] organized his desktop computer, including the backdrop or 'wallpaper', the placement and titles of folders, the titles of images and videos, and the presence of other non-illicit information."[109] All of this revealed "personal information about Mr. King", rendering the officer's act of viewing the screenshots a form of search. Following *Reeves*, the court held that King's wife could not consent to the search on his behalf and that it was unreasonable under section 8.[110]

The Alberta Court of Appeal treated the pictures the wife had taken on the USB drive as a further form of her *describing* or reporting the alleged offence.[111] Slater J held that "[t]he examination of the USB flash drive by the police was not an examination of any thing or place that belonged to or that was under the control of the appellant."[112] The trial judge's assessment was more plausible: *i.e.*, the officer did more than merely look at a picture of a picture. He looked at the *content* of the picture within a picture, giving him a substantial view of the content of the accused's computer. The difference this makes can be easily illustrated by considering screenshots given to police that depict not pornographic images but a private email, text exchange, or journal entry. Clearly in that case, an officer proceeding to *read* the texts would be doing more than 'receiving a report.'

King has since been cited in a later appellate decision for the proposition that "where information is brought to the police by an independent third party acting on its own initiative, and where the police merely receive and review it, there has been no search or seizure by the state which engages s. 8."[113] Trial courts have applied similar logic. In *Bear-Knight*, the court found the accused did not have a privacy expectation in the screenshot of a Facebook message the complainant brought to police.[114] Regardless of this, police receipt of the item from a third-party presenting it to them voluntarily meant that this could not be a search or seizure or, if it was, the party's consent sufficed to authorize police to conduct it.[115] In

---

[109] *Ibid* at para 24.

[110] *Ibid* at para 38, citing *Reeves*, *supra* note 4 at para 62.

[111] See *King* ABCA, *supra* note 105 at para 12.

[112] *Ibid* at para 18.

[113] *AK*, *supra* note 105 at para 34, involving screenshots of social media communications taken by an undercover US law enforcement agent and police in Canada receiving and reviewing the screenshots without a warrant.

[114] See *R v Bear-Knight*, 2021 SKQB 258 at para 56.

[115] *Ibid* at para 52, noting that the "complainant's actions in taking the screenshot, which the evidence suggests she voluntarily gave to the investigating officer, did not reflect surreptitious state action"; and at para 53: "the complainant had every right to provide

Lowrey, a mother and her 14-year-old daughter brought police the printout of a conversation the daughter had with the accused on Facebook.[116] The court held that despite the accused's "marginal expectation of privacy" in it, the daughter's consent was "sufficient to authorize the search [the officer had] undertaken."[117] In *Admurski*, the court held: "[t]here was no seizure by the police because the text messages were voluntarily turned over to the police by a concerned parent."[118] In *Phagura*, the complainant consented to police taking photos of a text exchange on her phone that she had with the accused.[119] The court found the accused lacked a reasonable privacy interest in the messages, but proceeded to address whether the complainant's consent provided sufficient authority for the search.[120] Since she and the accused had "an overlapping interest" in the exchange, it was not reasonable for the accused "to think or expect that Ms. M.K. would not be able to consent to provide such information to the police."[121] Her consent was "valid and sufficient for the police to obtain copies" of the exchange.[122]

There is certainly an appeal to the reasoning in these cases, arising from a sense of not wanting to needlessly impede civilians reporting a crime or police investigating it in good faith. An often-cited expression of this reasoning is found in a passage in *Orlandis-Habsburgo*.[123] In this case, an electricity company, Horizon, volunteered suspicious consumption data to police. The court held that police did not seize or search the data on receipt of it from Horizon because the company had a working arrangement with police from the outset, which rendered Horizon a state-agent. Horizon's initial investigative steps constituted an unreasonable search.[124] In *obiter*, however, Doherty JA considered what would have happened if Horizon were independent. Company officials could describe the suspicious data to police, which police could then include in an affida-

---

the police with the screenshot of the message she received. When she did so, she expressly consented to the police taking possession of it. In this context, there is some absurdity in the notion that the police should be expected to obtain a warrant to collect evidence in the lawful possession of a person who wishes, freely and voluntarily, to provide the evidence to the police without a warrant."

116 See *Lowrey*, *supra* note 106 at paras 8–9.

117 *Ibid* at paras 83–85.

118 *Admurski*, *supra* note 105 at para 4.

119 See *Phagura*, *supra* note 106.

120 *Ibid* at paras 56–57.

121 *Ibid* at para 62.

122 *Ibid*.

123 See *Orlandis-Habsburgo*, *supra* note 1 at para 34.

124 *Ibid* at paras 35–36, and 116–19.

vit for a warrant. Why, then, should things be different if an independent Horizon were to give police a copy of the data itself (as occurred here)?[125] Doherty J asserted:

> I have considerable difficulty with the submission that s. 8 is engaged if the police look at information in which an accused has a legitimate privacy interest, even if that information is brought to the police by an independent third party acting on its own initiative. On that approach, s. 8 would be engaged if a "whistleblower" took confidential documents belonging to her employer to the police to demonstrate the employer's criminal activity. Must the police refuse to look at the documents to avoid violating the employer's s. 8 rights?[126]

It may indeed be formalistic to require a warrant to permit an officer to read a document when he or she already knows what it contains. Yet this is essentially what happened in *Buhay*, *Cole*, and *Reeves*, where police already knew what the locker, laptop, or home computer contained.[127] Despite this, in each case the Court held that a third party's disclosure of the content did not negate the accused's privacy in it against the state. The answer in these cases—along with McLachlin CJ's *obiter* in *Marakah*—to Doherty JA's question 'must the police refuse to look?' is simply: yes. The broader explanation for why (canvased in the previous section and found in a host of Supreme Court decisions from *Hunter* to *Reeves*) is, in short, the high privacy interest in digital evidence can best be protected and societal expectations best met by holding police to certain standards before searching.[128]

A third group of cases centers the analysis on a persisting privacy interest, consistent with the Supreme Court's approach. A good example can be found in *Morgan*, where the accused was held not to have a privacy interest in messages he sent a woman he met only the night before and in texts he had sent to her on her mother's phone.[129] In *KA*, the court held that messages sent by two alleged pimps and human traffickers to their alleged sex worker and slave were not messages in which the accused had

---

[125] *Ibid* at para 33.

[126] *Ibid* at para 34.

[127] See *Buhay*, *supra* note 4 at paras 5–6; *Cole*, *supra* note 4 at paras 21–22; *Reeves*, *supra* note 4 at paras 6–7.

[128] See *Orlandis-Habsburgo*, *supra* note 1 at paras 36, 116, 118–19. The main holding is consistent with this line of reasoning. The police investigation began, Doherty JA held at para 36, when Horizon began observing suspicious patterns. Since the accused retained a privacy interest in the data, Horizon's use of it in coordination with police rendered it a search requiring authority (para 116). Police lacked authority, rendering the search unreasonable (paras 118–19).

[129] See *Morgan*, *supra* note 107 at para 105.

an objectively reasonable privacy interest, given the exploitive and tenuous nature of the relationships involved.[130]

Applying similar reasoning, other courts have come to the opposite conclusion—the accused did retain a privacy interest in the evidence turned over, resulting in a finding that a warrantless search of the evidence was unreasonable. One example can be found in the trial decision in *King*, noted earlier, involving police examination of screenshots.[131] Another can be found in *R v CM*, where the court held that the accused retained a privacy interest in messages sent to his former stepdaughter, which she gave to police.[132] The finding was based in part on the accused having known the recipient for a long time and standing in "a quasi-parental role towards her." [133] In *Devic*, a person responding to a Craigslist ad posted by a member of 'Creep Catchers' had a privacy interest despite not knowing their anonymous interlocutor.[134] In *Rafferty*, the court found a privacy interest in messages found on a phone a deceased son's father brought to police, incriminating the accused who was believed to be a dealer.[135]

The survey in this section was meant to show that lower courts are divided in their approach to assessing police receipt of digital evidence. The reasoning in support of diverging approaches is not compelling. It offers no response to the holdings from *Hunter* to *Reeves* that see the need for a warrant or other authority (aside from one-party consent) as an effective means of protecting the high privacy interest in the items at issue. By contrast, lower courts taking a principled approach demonstrate the viability of treating police receipt of texts and photos as a form of search, requiring a warrant, and the range of outcomes for which this still allows.

C. Conflicting Approaches Among Commentators

Commentators are also divided on questions raised by civilian disclosure of digital evidence. The scholars considered here agree that police

---

[130] See *R v KA and ASA*, 2022 ONSC 1241 [*KA and ASA*] at para 54 using these terms to describe the figures involved. For a further example involving a tenuous and exploitive relationship, see *Amdurski*, *supra* note 105. By contrast, in *R v Craig*, 2016 BCCA 154, a child luring case, the court finds a reasonable interest in messages to an underage girl by placing greater emphasis (at para 139) on the private nature of the messages than on the exploitive nature of the relationship.

[131] See *King* ABPC, *supra* note 107 at para 65.

[132] See *R v CM*, 2022 ONCJ 372 at para 41.

[133] *Ibid* at para 37.

[134] See *R v Devic*, 2018 BCPC 318 at para 46.

[135] See *R v Rafferty*, 2018 ONCJ 881 at para 32.

engage section 8 on receipt of evidence from a civilian. But each of them offers a position that diverges from the Court's principled approach in suggesting that *civilian* disclosure renders the situation different from other searches and seizures police conduct. In their view, police are justified to search a text exchange or an email on one party consent, reasonable suspicion, or no grounds or consent at all. These views diverge from McLachlin CJ's position in *Marakah* that police should need a warrant before conducting a search, and also from the Court's decisions (surveyed in Part I) holding a warrant to be necessary to render a search reasonable in a variety of scenarios. As the survey in Part I showed, the Court consistently found a warrantless search or seizure unreasonable without factoring in *how* police obtained the item. I argue that none of the alternative views canvassed here offers a compelling argument for diverging from McLachlin CJ's approach to text messages or from the Court's principled approach more broadly.

Steven Penney weighed in on the debate after the Supreme Court had decided *Marakah* but before it had decided *Reeves*.[136] Professor Penney lauded the Court of Appeal's approach in *Reeves* to shared privacy interests and its application of this approach to police entry into the Reeves' home (with spousal consent).[137] Penney supports LaForme JA's argument that a co-resident cannot reasonably expect their housemate to never invite an agent of the state into the home, since "the other might have a legitimate interest in consenting to entry by law enforcement into common spaces from time to time."[138] The rule, in Penney's view, should apply to text messages because "while it is sometimes difficult to decide whether residential spaces are shared or exclusive, received text communications are always shared between the parties."[139] On this basis, Penney proposes a rule permitting third parties "including victims of and witnesses to criminal activity, to consent to searches of their devices for incriminating messages sent to them" on the basis that it would "further public safety and crime control without unduly diminishing the privacy of electronic communications."[140]

Penney offers a cogent alternative to the approach suggested in *Marakah* and *Reeves*. Yet he provides no support for his assertion that permitting police to rely on the consent of the recipient of a text to read

---

136 See Penney, *supra* note 11 at 11–13; *Marakah*, *supra* note 4; *Reeves*, *supra* note 4.

137 As noted earlier, a majority of the Supreme Court of Canada on appeal explicitly declined to address the issue of police authority to enter the home; see *Reeves*, *supra* note 4 at para 23.

138 *R v Reeves*, 2017 ONCA 365 at para 48, cited in Penney, *supra* note 11 at 10.

139 Penney, *supra* note 11 at 13.

140 *Ibid*.

the messages would further public safety without unduly diminishing privacy in text messages generally. This is a value judgement—a reasonable but different view of where to strike the balance between law enforcement and individual privacy from the one McLachlin CJ offers in *obiter* in *Marakah* canvassed earlier. Penney shares the view of Moldaver and Côté JJ in *Marakah* that when it comes texts messages the balance is best struck in favour of one-party consent. The Chief Justice's preference for a warrant in this case need not be taken to mean that nothing short of a warrant requirement would strike an appropriate balance of interests here. Yet, the majority's position in *Marakah* and *Reeves*, holding that police need a warrant to search text messages or a computer suggests that police need *something more than third party consent* to render state interference reasonable, given the high degree of privacy in text messages and the goal of avoiding unnecessary intrusions before they occur.[141] Short of a warrant, the reasoning in these two cases implies, privacy in digital communications would indeed be unduly diminished.

Put another way, a rule permitting police to rely on one-party consent to a text-exchange would have the effect of permitting state intrusion into immensely private spaces on the whim of a disgruntled recipient. Penney might counter that obtaining reasonable grounds will often involve an officer hearing so much about the content of an exchange that it would hardly "differ substantially from police looking at the messages themselves".[142] That may indeed be the case in some instances. But this is really a form of the 'why bother getting a warrant?' argument addressed above.

Simon Stern offers a subtle analysis of *Marakah*, informed by a background in media theory and search law on other forms of written communication.[143] He takes issue with Supreme Court's holding in *Marakah* that if a sender retains a reasonable privacy interest in text messages, police need a warrant on probable grounds to seize them. He sees a better alternative in the rule crafted in *R v Fearon*.[144] The Court in *Fearon* held that under certain conditions, police may conduct a warrantless but limited search of a phone incident to arrest. In Stern's view, if in this context the "showing of a heightened privacy interest as to a certain item makes no difference" and "any evidence [police] collect is admissible, whether it is a

---

141 Texts may not hold as much information as computers, but as McLachlin CJ noted in *Marakah*, *supra* note 4 at para 37, "[e]lectronic conversations … are capable of revealing a great deal of personal information."

142 Penney, *supra* note 11 at 14.

143 Stern, "Textual Privacy," *supra* note 12, making no reference to *Reeves*, *supra* note 4, in his article.

144 2014 SCC 77 [*Fearon*].

bus transfer or a personal diary",[145] a police power to seize and search text messages volunteered to them on reasonable suspicion should be reasonable.[146]

Stern misreads *Fearon*. He correctly notes that the majority assumed a warrantless search would "serve important law enforcement objectives" including "identifying accomplices or locating and preserving evidence that might otherwise be lost or destroyed."[147] But the key point for the majority was that police on arrest need to conduct a search for these purposes *promptly*—and their need to do so is *pressing*.[148] In the view of the dissent, it was not.[149] Nor did it seem pressing to the US Supreme Court in *Riley v California*, decided earlier that year.[150] For the dissent in *Fearon* and the USSC in *Riley*, police could wait to search for evidence, and concerns about nefarious uses of a phone following an arrest were no more than speculative and did not outweigh the high privacy interest in a device.[151] Stern entirely overlooks this debate and offers no analogue to the balancing involved in police receiving a text exchange from a recipient. What pressing need does law enforcement have in reading a text or email a civilian has brought them *promptly*, rather than waiting to obtain a warrant? McLachlin CJ's treatment of the scenario in *Marakah* as-

---

145 Stern, *supra* note 12 at 434.

146 *Ibid* at 435.

147 *Fearon*, *supra* note 144 at paras 48–49; Stern, *supra* note 12 at 434.

148 The passage from *Fearon*, *supra* note 144 just cited (in para 49) makes this explicit. Cromwell J emphasizes the importance of police being able to carry out a search "promptly" by using the words "prompt" and "promptly" six times in the paragraphs assessing the state interest in search (paras 45-49). At para 49, he contrasts the lack of urgency in obtaining a DNA sample (justifying a warrant requirement) or a strip search in the field from the need to search a phone "promptly" on arrest to avoid losing evidence or allowing police to "identify and mitigate risks to public safety".

149 See *Fearon*, *supra* note 144 at paras 140–43. See *ibid* at para 153, Karakatsanis J: "In my view, the weighty privacy interest an arrested person has in her cell phone will outweigh the state interest in performing a warrantless search incident to arrest, except in exigent circumstances."

150 See *Riley v California*, 134 S Ct 2473 (2014) at 2485–89.

151 See *Fearon*, *supra* note 144 at para 141, Karakatsanis J holding: "The mere possibility that a phone *could* have been used to summon backup does not justify a search incident to arrest any more than the theoretical possibility that the suspect's home *could* contain accomplices justifies a search of the home." She notes at para 144: "The mere *possibility* that evidence on the cell phone could be remotely deleted should not justify a search." See also *Riley*, *ibid* at 2486, holding that while phones might be wiped remotely or used to conceal evidence, there was no evidence that "either problem is prevalent or that the opportunity to perform a search incident to arrest would be an effective solution."

sumes no such need. Short of a text alleged to contain an *imminent* threat of serious harm, there is no case for urgency on the part of police.[152]

Hamish Stewart commented on McLachlin CJ's *obiter* in *Marakah* in the context of an essay on a reasonable expectation of privacy as a right.[153] Stewart's comments are prefaced by a consideration of Moldaver J's observations on the consequences of the majority's holding in *Marakah*. Finding a continuing privacy interest in a message by a sexual predator who threatens to kill a child leads, in Moldaver J's view, to the absurd result of the predator's section 8 rights being engaged when a parent turns over the messages to police.[154] Stewart agrees with Moldaver J that this result is "untenable," but contends that Moldaver J is mistaken in thinking it flows from the majority's holding. The majority held that the predator may have a reasonable expectation of privacy against the state but not against the victim. If the victim or her parents "voluntarily provide the text messages to the police", Stewart contends, "section 8 of the *Charter* would not be engaged because, being private actors, they have no *Charter* duties toward the suspect, just as section 8 is not engaged where a complainant shows a threatening letter or email to the police."[155] Stewart suggests, however, that police might need a warrant or other authority to "obtain … a complete record of the exchanges between the suspect and the complainant."[156] He acknowledges McLachlin CJ's differing view in *obiter* in *Marakah*, but assumes she was merely framing police receipt of threatening texts on civilian disclosure as a search in that passage "for the sake of argument."[157] He offers the "tentative view" that police would not need a warrant to read threatening messages, since disclosure would not constitute a search.[158]

Stewart's view on civilian disclosure of private messages runs contrary to the Supreme Court's holdings on receipt and transfer. It also runs

---

152 An imminent and serious threat would give rise to exigent circumstances, authorizing police to search without a warrant, under *Criminal Code*, s 487(11).

153 See Stewart, *supra* note 13 at 46–47.

154 See *Marakah*, *supra* note 4 at 168; Stewart, *ibid* at 46.

155 Stewart, *supra* note 13 at 46.

156 *Ibid* at 47.

157 *Ibid*. A reading of the entire passage of McLachlin CJ's opinion in *Marakah, supra* note 4 at paras 50–52, where the *obiter* appears, supports the view that she does more than assume for the sake of argument that civilian receipt would be a search in this instance. She offers the opinion as the first of three scenarios, each involving a framing of receipt as a search—suggesting that this follows necessarily upon a finding of a reasonable privacy interest in the messages turned over and police receipt of them for an investigative purpose.

158 Stewart, *supra* note 13 at 47.

contrary to the Court's holding on third party consent to search items over which parties share an interest, noted earlier. Stewart offers no argument for why police do not conduct a search when a parent shows an officer the threatening text itself but do conduct a search when the officer proceeds to read the entire exchange. An approach consistent with Supreme Court jurisprudence on privacy and receipt would be to suggest that a threatening text or email could still engage a privacy interest, but an imminent threat would provide police authority to carry out a warrantless search in exigent circumstances.[159] Alternatively, as McLachlin CJ suggests in *Marakah*, a court might find that police intruded on a privacy interest in reading a text containing an alleged threat, and doing so without authority violated section 8. But given the technical and limited nature of the breach, the evidence would be admitted under section 24(2).[160]

A final criticism to note here pertains to McLachlin CJ's assumption that police could in most cases readily obtain a warrant to read a private exchange based on a complainant's description of its contents. Michelle Biddulph calls this into question.[161] Under section 487(1) of the *Criminal Code*, an affiant seeking a warrant must establish probable grounds that an offence has been committed and evidence of it will be found in the place to be searched.[162] An affiant would need to be somewhat detailed, and an officer's description of what the complainant said about the texts would be hearsay. In some cases, this may not suffice for probable grounds.[163] She thinks a warrant requirement places "needless and im-

---

159 See *Criminal Code*, s 487(11). See also *R v Paterson*, 2017 SCC 15 [*Paterson*] at para 33, interpreting 'exigent circumstances' to require "urgency" in (the similarly worded) section 11(7) of the *Controlled Drugs and Substances Act*, SC 1996, c 19.

160 See *Marakah*, *supra* note 4 at para 52. A third possibility [canvassed in Part II above] is that a court might find that since a threat constitutes the *actus reus* of an offence, it would not attract an objectively reasonable expectation of privacy: see e.g. *R v Patterson*, 2018 ONSC 4467 at para 13 [*Patterson*], applying this reasoning to texts involving the offence of child luring.

161 See Michelle Biddulph, "The Privacy Paradox: *Marakah*, *Mills*, and the Diminished Protections of Section 8" (2020) 43:5 Man LJ 161.

162 See *Criminal Code*, s 487(1).

163 See Biddulph, *supra* note 161 at 177–78; at 178 Biddulph cites authority for the proposition that "[w]hile hearsay is commonly used in ITOs, the hearsay information must be properly sourced in order to be deemed adequate. This generally means that the affiant must identify the source of the information — in this scenario, the complainant — as well as any other relevant information that may bear on the source's credibility." She cites in support: *R v Vaz*, 2015 BCSC 728 at paras 15–16; *R v KP*, 2011 NUCJ 27 at para 83; *R v Sparks*, 2015 NSSC 233 at paras 10–11; *R v Patterson*, 2014 NSPC 101 at para 20; *R v Pontes*, 2014 BCPC 19 at para 12.

possible burdens for the police... to know something that they already knew."[164]

Biddulph raises important concerns. In many cases, police may face a real burden in obtaining a warrant. But the burden is not a needless one. Missing in Biddulph's analysis is a consideration of the rationale for putting police to the trouble of obtaining a warrant before proceeding to search presumptively private messages. As canvassed earlier, imposing a standard affords a measure of assurance to everyone that the state will not intrude on private communications without certain steps being taken. This accords with a wider societal expectation against state interference in private spaces generally. Far from being pointless, we impose a burden on police in these cases precisely in order to make it more difficult for them to intrude.

D. Remaining Questions and How They Should be Resolved

The challenge for commentators and judges is to understand why a brief text exchange that a civilian hands over to police—even only a single page or two—is *not* different from a closed container, a locked cabin, or a book titled 'secret journal' that police might encounter in the course of an investigation. In the latter cases, it is easy to see how police proceeding to open or analyze the object would clearly constitute an intrusion of privacy. It is easy to overlook how the same can be said to happen the instant an officer begins to review, peruse, or analyze a short exchange, email, or photo. Courts and commentators alike fail to distinguish between the officer having knowledge of the content of an item and an officer reading or reviewing the item itself. They assume that because in some cases this may amount to a distinction without a difference, no distinction should be drawn in *any* case. Yet, as the majority held in *Marakah*, a text exchange can engage a high degree of privacy.[165] So might a photo or an email. The reasoning about texts in *Marakah* suggests that if a suspect retains a privacy interest in a communication against the state, police conduct a search if they review it—even if police obtain it from a third party who volunteers it, even if it is brief, and even if police have a good sense of what it contains.

However, in the absence of a Supreme Court decision directly on point, the Court has yet to decide two discrete issues raised here: do police conduct a seizure when they take custody of a text, email, or photo when a civilian volunteers it, and do they conduct a search if they proceed to review it, even in a cursory fashion?

---

[164] Biddulph, *supra* note 161 at 178.

[165] See *Marakah*, *supra* note 4 at para 35.

Turning to the first of these questions, McLachlin CJ's *dicta* in *Marakah* and the Court's holding in *Cole* assume that, when a civilian has described the incriminating content of an item, police are authorized to take custody of it briefly, to obtain a warrant.[166] In *Reeves*, the officer testified to not believing he had reasonable grounds to seize the computer under the 'plain view' provisions of the *Criminal Code*,[167] and the Court held the officer could not rely on the spouse's consent. A reading of the three cases suggests that an officer carries out a seizure under section 8 when they receive an item a civilian volunteers in which the accused retains a privacy interest, even a text, email, or photo in which the civilian has a shared interest. A possible source of authority for the seizure can be found in the plain view powers of the *Criminal Code*, which permits an officer in the execution of her duties (*i.e.*, receiving a report) to seize an item they reasonably believe will afford evidence of an offence.[168] Another source would be the *Code* power to seize in exigent circumstances, though this would apply in a narrower set of circumstances.[169]

Turning to the second question, whether police conduct a search if they proceed to review a text exchange a recipient discloses—even briefly—should turn on the question of privacy and not consent. It should turn on whether the accused retained a reasonable privacy interest in the message against the state, and thus not on the identity of the party disclosing it, or the fact that a civilian with a shared interest in it voluntarily disclosed it rather than police having asked for or taken it. McLachlin CJ's *obiter* in *Marakah* offers a blueprint for a future holding consistent with the Court's earlier jurisprudence. If, applying the four-part test for a privacy interest in *Marakah*,[170] a suspect is held to retain a reasonable privacy interest in a text-exchange turned over by a complainant, in keeping with *Cole* and *Reeves*, the complainant's consent should not serve as authority for a search.[171] Even a victim of 'cyber abuse' turning over a chat to police would not, in McLachlin CJ's view, authorize police to read the texts without a warrant.[172]

Taking this approach, whether civilian disclosure of digital communications engage section 8 will likely be determined by deciding whether the

---

166 See *ibid* at para 50; *Cole*, *supra* note 4 at para 65.

167 See *Reeves*, *supra* note 4 at para 21, considering the plain view power in the *Criminal Code*, s 489(2).

168 See *Criminal Code*, s 489(2)(c).

169 See *Criminal Code*, s 487.11; *Paterson*, *supra* note 159.

170 See *Marakah*, *supra* note 4 at para 11.

171 See *Cole, supra* note 4 at paras 74–79; *Reeves*, *supra* note 4 at paras 40–58.

172 See *Marakah*, *supra* note 4 at para 50.

accused retains an objectively reasonable expectation of privacy in the message. This should involve asking whether a reasonable person in the position of the accused might have accepted as reasonable the form of disclosure made in that case to the state if it were presented to them as a hypothetical. Lower courts have posed the question in precisely these terms. For example, can a male in an exploitive relationship with an adolescent female reasonably expect her not to reveal to parents or police communications that urge her to engage in criminal activity?[173] There have been ample criticisms of the Court's decision in *Marakah* to not declare that all personal digital communication gives rise to a reasonable expectation of privacy (in contrast to all private conversations surreptitiously recorded by a state agent).[174] Taking a case-by-case approach to whether an exchange is private may appear to run contrary to the Court's earlier jurisprudence affirming a normative and content-neutral approach to assessing reasonable expectation of privacy.[175] (In this author's view, *Marakah*'s case-by-case approach *is* a normative inquiry, one that looks not at the content of a communication but at its form or nature.) Setting that debate aside, however, the point here is that concerns about the absurdity of police needing a warrant or civilian disclosure engaging section 8 belong in the assessment of whether the accused retained a reasonable privacy interest in the communication—and not, if he did have an interest, whether receipt constituted a search or seizure.

---

[173] This was essentially the question in *Amdurski*, *supra* note 105, where the court found that the accused did not have a reasonable expectation of privacy in texts sent to the complainant in light of his knowledge that she was under the age of consent and he communicated with her to arrange sex for money. In *Patterson*, *supra* note 160, a case involving child luring of a 15-year-old boy, the court held at para 26: "A reasonable person in Mr. Patterson's position would foresee the possibility that the victim's parents could be monitoring his Facebook activities. Or that the victim might disclose the conversations to a trusted friend. Or that the victim might mistakenly leave his Facebook page open on the family computer where the communications could be discovered by a parent or sibling." The question in *KA and ASA*, *supra* note 130 at para 63, was whether "alleged pimps and human traffickers" had a reasonable privacy interest in "text messages with their alleged sex worker and slave".

[174] See e.g. Stern, *supra* note 12 at 432; Stewart, *supra* note 13 at 45–47.

[175] See *Duarte*, *supra* note 21 at 47–48; *Wong*, *supra* note 58 at 45. See also Martin J's opinion in *R v Mills*, *supra* note 25 at 113–14 taking issue with Brown J's opinion in this case that "it is not reasonable for an adult to expect privacy when communicating with a vulnerable child who is a stranger." Martin J contends "this position reintroduces the 'loss of control due to risk of disclosure' analysis that this Court recently rejected in *Marakah*."

Conclusion

Courts are increasingly relying on evidence disclosed by civilian recipients of texts, email, and other digital evidence volunteered to police. Courts and commentators have found it challenging to apply to this situation the Supreme Court's long-standing, clear, and consistent jurisprudence on what constitutes a search or seizure and when it will be reasonable. In many cases, judges and scholars have been quick to assume that since a piece of evidence turned over is brief or slight (a one-page exchange, a screenshot) and since police have been told of its contents, they do nothing to interfere with any possible continuing privacy interest a suspect may have if an officer proceeds to peruse it. They do not see the item as engaging a significant privacy interest, if any, or the perusal as an investigative technique. And more to the point, if it were put to them that even a brief text possibly containing a threat still engages a privacy interest and perusing it is a search, they would ask 'why should it matter'? Why should police need authority to conduct this search when they already know what a text contains and the exchange or email is so brief?

This article has sought to demonstrate that the Court has consistently approached the question of whether a search and seizure has taken place not by asking who gave what to whom and why. In every case, the Court has asked instead whether an accused retained a reasonable privacy interest against the state in the item at issue and whether in taking, receiving, or perusing the item, the police had an investigative purpose. The Court's holdings on digital evidence, including *Cole*, *Reeves*, and *Marakah* suggest that we may retain a high degree of privacy in even a brief or seemingly slight piece of evidence such as a short exchange or a screenshot of some portion of the content of a device, and that police review of it entails a search.

Judges and commentators have also overlooked the rationale for insisting that police obtain a warrant or other authority to render a search in these circumstances reasonable. In many cases, this will seem redundant or pointlessly formalistic, given the knowledge the officer already possesses at the time she proceeds to peruse a brief text. The point is not to make her work unnecessarily difficult. As the Supreme Court has held in numerous cases canvassed here where police already the know what a search will likely reveal, putting police to the trouble of obtaining a warrant or other authority affords everyone in Canada the assurance that the state will not interfere with a reasonable expectation of privacy unless certain standards are met. Digital communications are ubiquitous and a central part of our lives. The assurance of privacy from state interference may seem abstract and remote to many, but its absence would affect us all.