The Privacy Paradox: *Marakah*, *Mills*, and the Diminished Protections of Section 8

MICHELLE BIDDULPH *

ABSTRACT

The Supreme Court of Canada's decision in *R v Marakah* is a landmark decision under section 8 of the *Charter*, as it extended constitutional protection to some electronic communications that are no longer in the control of the sender. In other words, the presence or absence of control is no longer determinative.

This article challenges the understanding of *Marakah* as a progressive decision, suggesting that *Marakah* has created a privacy paradox. By significantly expanding the scope of section 8 of the *Charter*, the Court in *Marakah* has created a right that is both extremely broad and practically illusory. In order to deal with the practical challenges resulting from the decision in *Marakah*, this article suggests that courts will deal with *Marakah* by diluting current principles under section 8 in order to avoid absurdities and undesirable results.

The Supreme Court's majority decision in the 2019 decision of *R v Mills* illustrates the privacy paradox. Unable to rely on the accused's lack of control over communications as a determinative factor, the majority in *Mills* abandoned decades of jurisprudence under section 8 of the *Charter* to reach its desired result. The new concept of privacy as "relationship-based" places courts in the business of conducting a post facto assessment of which relationships are entitled to privacy.

* B.A. (Saskatchewan), J.D. (Saskatchewan), Associate Lawyer, Greenspan Humphrey Weinstein LLP. I thank Terry Skolnik for his comments on several drafts of this article, Jonathan Finlay for his review of multiple drafts, and the two anonymous reviewers for their helpful suggestions. I also thank the editors of the Manitoba Law Journal for their hard work. All errors are my own.

As shown by *Marakah* and *Mills*, those who seek progressive and idealistic development of *Charter* principles through Supreme Court jurisprudence should be careful what they wish for. The most well-intended decision can have very unintended results.

Keywords: privacy; text messages; judicial reasoning; precedent; *Charter of Rights and Freedoms*; Supreme Court of Canada

I. Introduction

In *R v Marakah*,[1] a majority of the Supreme Court held that the sender of a text message may retain a reasonable expectation of privacy in the message despite the absence of control over the use of the message by the recipient, thereby precluding the police from accessing that text message without prior judicial authorization. This reasonable expectation of privacy would prevent all unauthorized searches and seizures of the message, whether on the sender's device, the recipient's device, or some other locale.

The issue in *Marakah* seemed deceptively simple. After all, if the police cannot search an accused person's phone without a warrant to obtain incriminating text messages that the accused person has sent, why should the police be able to achieve that exact same result by searching the recipient's phone without a warrant? On policy grounds, the answer was clear. But the implications of that answer, as shown by *Mills*, are troubling.

This article suggests that the effect of the majority's decision in *Marakah* was to create what I have termed as a privacy paradox. The majority's decision created a section 8 right that was, paradoxically, extremely broad and practically illusory. It created an extremely broad section 8 right because the sender of information can always claim a subjective intention to shield that information from the prying eyes of the state, regardless of whether the recipient of the information has any legal obligation to keep that information confidential. Based on the majority's reasoning in *Marakah*, it is difficult to imagine a scenario where that subjective expectation of privacy is not objectively reasonable because control is no longer a predominant factor in assessing the objective reasonableness of that expectation of privacy. Unmoored from the concept of control, it appears that, based on *Marakah*, a truly credible subjective expectation of privacy in an electronic

1 2017 SCC 59 [*Marakah* 2017].

communication sent to another individual[2] will almost automatically result in that subjective expectation being objectively reasonable.

But this expansion creates a paradox. By finding that virtually everyone holds a reasonable expectation of privacy in their electronic communications sent to a designated recipient, the majority implied in *Marakah* that the police will always require prior judicial authorization or must conduct a lawful, warrantless search in order to view those communications on the third party's device. The majority suggested that these problems can be addressed by the existing principles governing warrants, warrantless searches, and section 24(2) of the *Charter*.[3] However, if a court were to truly apply these principles to communications in the possession of third parties, two results are likely: either the courts will be forced to dilute the protections of section 8 of the *Charter* for all, or else the privacy right established in *Marakah* becomes meaningless. In other words, by expanding the scope of section 8 of the *Charter*, the majority's decision may have rendered this right less meaningful.

After setting out the privacy paradox created by *Marakah*, I suggest that the existence of this privacy paradox is demonstrated by Justice Brown's majority[4] opinion in *R v Mills*.[5] His opinion attempts to rein in *Marakah* by adopting a results-oriented approach to the objective reasonableness of Mr. Mills' expectation of privacy, finding no objectively reasonable expectation of privacy without actually applying the test set out in *Marakah*. He justified this through a "relationship-based" understanding of a reasonable

---

2 There is, of course, no suggestion here that a claimed subjective expectation of privacy in any electronic communication would automatically be objectively reasonable. For example, a person who tweets to their followers on Twitter could not credibly claim a subjective expectation of privacy in the information that the accused intentionally broadcast publicly. Similarly, an email sent to multiple people, rather than one designated recipient, may lose any credible claim to a subjective expectation of privacy. To avoid becoming mired in the conceptual difficulty with group communications and expectations of privacy, I have limited my analysis to the two-party communication situation which was at issue in both *Marakah* and *Mills*, as it is this situation that is most common in section 8 cases and will likely pose the most problems for accused persons and law enforcement.

3 *Marakah* 2017, *supra* note 1 at paras 46–53.

4 It is something of a misnomer to describe Justice Brown's opinion as the majority, given that the Court was unanimous in dismissing the appeal. However, as Justice Brown's opinion gathered the largest number of concurrences, I have termed it as the majority in this article for ease of reference.

5 2019 SCC 22 [*Mills*].

expectation of privacy, which acts as a proxy for the notion of control that was rejected in *Marakah*. I show why this approach is inconsistent with the Court's prior case law and appears to abandon the content-neutral approach to section 8 which has been consistently affirmed by the Supreme Court since the *Charter*'s inception.

The purpose of this article is not to chart the future course of section 8 of the *Charter*, nor to provide a theoretical analysis of the concepts of privacy that the Supreme Court has espoused in either *Marakah* or *Mills*. Others have written extensively on these topics and I cannot claim to improve their ideas.[6] Instead, this article is about how well-intended judicial decisions can have very unintended results. The Court's decision in *Marakah* appeared to display a rather myopic understanding of the implications of its reasoning: the majority rejected any suggestion that its decision could have any broader negative implications for section 8 of the *Charter* in general.[7] Similar assertions were made by the majority opinion in *Mills*.[8] Yet proclaiming a decision to be narrowly confined to the facts of the case, with no broader jurisprudential meaning, does not necessarily make it so. Like it or not, Supreme Court decisions tend to have major precedential effect.[9] By

---

6 Other authors have done a commendable job of theoretically analyzing *Marakah* and, to a lesser extent, *Mills*. For academic commentary on these decisions, see: Steven Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap" (2018) 56:1 Alta L Rev 1; Ryan Mullins, "*R v Jarvis*: An Argument for a Single Reasonable Expectation of Privacy Framework" (2018) 41:3 Man LJ 77; Simon Stern, "Textual Privacy and Mobile Information" (2018) 55:2 Osgoode Hall LJ 398.

7 See e.g. *Marakah* 2017, *supra* note 1 at paras 49–53, responding to criticisms laid out in Justice Moldaver's dissenting opinion.

8 Justice Brown took a similar approach in responding to criticisms from Justice Martin's dissent in *Mills*, rejecting the assertion that the narrow reasoning in his opinion could have broader negative effects. See *Mills*, *supra* note 5 at para 30.

9 Indeed, it appears that since *Mills* lower courts have relied on it to deny section 8 protections to unsavoury or abusive communications emanating from the accused. See e.g. *R v Heppner*, 2019 MBPC 73 at para 8 [*Heppner*] (holding that the accused's expectation of privacy in his email communications with the complainant, a vulnerable person, was not objectively reasonable because she was a vulnerable person); *Estrella Llaneza c R*, 2019 QCCQ 3012 at para 37 (relying on *Mills* to hold that, despite the statement at para 50 of *Marakah*, *supra* note 1 that the police require a warrant to view private communications even where they are voluntarily disclosed, there is no objective expectation of privacy in a communication to a victim that is voluntarily provided to the police). At the time of writing (May 2020), there does not appear to yet be an appellate decision directly considering the correctness of a lower court's application of *Mills* in this context. I have not considered the decisions applying *Mills* in the context of the new section 278.92 of the *Criminal Code* and a complainant's reasonable

blinding itself to the precedential effect of *Marakah*, the Supreme Court ended up with *Mills*. And by blinding itself to the precedential effect of *Mills*, the Supreme Court may have unwittingly set itself down a path that will result in diluted privacy protections for all.

II. The Decision in *R v Marakah*

A. The Facts

In mid-2012, the Toronto Police Service began an investigation into persons who had legally purchased firearms over a short period of time. This investigation led them to Andrew Winchester, who had purchased 45 firearms over a six-month period. Information from a confidential informant implicated Mr. Marakah in the investigation. The police obtained four search warrants: one for Mr. Winchester's apartment; one for Mr. Winchester's girlfriend's apartment; one for Mr. Winchester's vehicle; and one for Mr. Marakah's apartment.[10] Mr. Winchester was arrested, and an iPhone was seized from his front pocket incident to arrest. It was not searched at the scene of the arrest. The police then searched Mr. Winchester's apartment and car and found a number of firearms.[11] Both of the accused's phones were seized and sent to the Tech Crimes division for further analysis, though no warrants were obtained in respect of the searches of either phone. Tech Crimes extracted the information from both phones and provided them to the police.[12] Numerous text messages between Mr. Marakah and Mr. Winchester were found on both phones, which implicated both Mr. Marakah and Mr. Winchester in firearms trafficking.[13]

B. The Supreme Court Judgement

Mr. Marakah appealed as of right to the Supreme Court of Canada,

---

expectation of privacy in records sought or held by the accused, as the interests of the accused in protecting privacy against the state are vastly different from the interests of a sexual assault complainant in protecting privacy against the accused. The comparison between the application of *Mills* to section 8 claims by the accused and the application of *Mills* to privacy claims under section 278.92 is fascinating, but ultimately outside the scope of this article.

10 *R v Marakah*, 2014 ONSC 7580 at para 10 (*Voir Dire* Judgment).

11 *Ibid* at para 14.

12 *Ibid* at paras 20–21.

13 *R v Marakah*, 2016 ONCA 542 at para 1.

which ultimately allowed his appeal.[14] Chief Justice McLachlin wrote for the majority, with Justices Abella, Karakatsanis, and Gascon concurring. Justice Rowe wrote a separate concurring opinion, while Justice Moldaver dissented, with Justice Côté concurring.

Chief Justice McLachlin held that Mr. Marakah had a reasonable expectation of privacy in the text messages that were found on Mr. Winchester's phone. She stated that the subject matter of the search was not Mr. Winchester's phone, nor the contents of that phone. The subject matter of the search was, instead, Mr. Marakah's "electronic conversation" with Mr. Winchester.[15] Mr. Marakah had a direct interest in the subject matter of the search, given that he was a participant in the electronic conversation.[16] He also had a subjective expectation of privacy in the subject matter of the search, as he had testified as to his subjective expectation that the contents of the conversation would remain private.[17] The only issue to be determined was whether his subjective expectation of privacy was objectively reasonable.

Chief Justice McLachlin considered three factors that were relevant to assessing whether Mr. Marakah's expectation of privacy was objectively reasonable: (1) the place of the search; (2) the private nature of the subject matter; and (3) control over the subject matter. With respect to the first factor, she stated that, regardless of whether the "place" of the search is characterized as a metaphorical "chat room" between two individuals or as the physical device through which the messages are accessed or stored, "it is clear that the place of the text message conversation does not exclude an expectation of privacy."[18]

With respect to the second factor, the private nature of the information, Chief Justice McLachlin noted that "the focus is not on the actual content of the messages the police have seized, but rather on the potential of a given electronic conversation to reveal personal or biographical information."[19] She stated that text message is an extremely discrete form of communication "capable of revealing a great deal of personal information" and that it is, therefore, "reasonable to expect these private interactions — and not just the

---

14 *Ibid* at para 87. He was convicted after trial and a majority of the Court of Appeal for Ontario dismissed his appeal, with LaForme JA dissenting.

15 *Marakah* 2017, *supra* note 1 at para 17.

16 *Ibid* at para 21.

17 *Ibid* at para 23.

18 *Ibid* at para 30.

19 *Ibid* at para 32.

contents of a particular cell phone at a particular point in time — to remain private."[20]

Finally, with respect to the third factor — control — Chief Justice McLachlin held that a person does not lose control over information for the purpose of section 8 "simply because another person possesses it or can access it."[21] Even though Mr. Marakah accepted the risk that, by sharing information with Mr. Winchester, the information could be disclosed to third parties, this did not mean that Mr. Marakah ceased to have control over the information. Instead, Chief Justice McLachlin held that "[b]y choosing to send a text message by way of a private medium to a designated person, Mr. Marakah was exercising control over the electronic conversation" and the risk that Mr. Winchester could have disclosed it did not negate the reasonableness of his expectation of privacy "against state intrusion."[22] Chief Justice McLachlin concluded that Mr. Marakah did have a reasonable expectation of privacy in the electronic conversation, held that the evidence ought to be excluded under section 24(2), allowed the appeal, and entered acquittals on all counts.[23]Justice Rowe, concurring, agreed with Chief Justice McLachlin that Mr. Marakah had a reasonable expectation of privacy in the impugned text messages. However, he echoed some of Justice Moldaver's concerns regarding the policy implications of this decision. Justice Rowe ultimately stated that all of these policy concerns could not be resolved within the confines of this case but warned that "principle and practicality must not be strangers in the application of s. 8."[24]

Justice Moldaver wrote a lengthy dissent. He agreed that text message conversations are inherently private in nature, such that the police's decision to view the text messages on Mr. Winchester's phone amounted to a search for the purpose of section 8.[25] However, the question of whether a search has occurred is different from the question of whether a person has standing to challenge the legality of that search. He held that Mr. Marakah lacked standing to challenge the legality of the search of the text messages because Mr. Marakah lacked a reasonable expectation of privacy in them. This was because, in his view, Mr. Marakah lacked any control over those

---

20 *Ibid* at paras 35–37.
21 *Ibid* at para 41.
22 *Ibid* at para 45.
23 *Ibid* at paras 72–73, 82.
24 *Ibid* at para 89.
25 *Ibid* at para 106.

text messages.

The notion of control was central to Justice Moldaver's dissent. He stated that, in assessing standing, control "plays an integral role" in defining the strength of the connection between the claimant and the subject matter of the search.[26] This remains integral in the context of informational privacy because of "the ease with which information can change from private to public in nature, depending on the context."[27] An individual need not demonstrate absolute control over the information in order to demonstrate a reasonable expectation of privacy, but, in Justice Moldaver's view, the individual must retain some measure of control over that information in order to retain a reasonable expectation of privacy in it.[28]

Control may also be constructive in nature: for example, a legal obligation of confidentiality imposed on the recipient of information vests constructive control in the individual from whom that information originated. Thus, a client retains constructive control over information shared with a lawyer, or a patient retains constructive control over private information shared with their physician. However, Justice Moldaver held that such constructive control does not exist "where the information in question is under the exclusive control of another person[, as] an interest in the subject matter and a personal relationship with that person does not suffice."[29] He, therefore, found no section 8 breach and would have dismissed the appeal.[30]

III. The Privacy Paradox

The majority decision in *Marakah*, which found that the sender of a communication retains a reasonable expectation of privacy even in the absence of control over the communication, creates a paradox. The plurality decision in *Mills*, authored by Justice Brown and ultimately followed by lower courts,[31] illustrates this paradox. The privacy paradox rests on two premises: first, the majority decision in *Marakah* vastly expanded the scope of section 8 of the *Charter*; and second, by doing so, it will dilute the

---

26 *Ibid* at para 122.
27 *Ibid* at para 125.
28 *Ibid* at paras 127–29, 133.
29 *Ibid* at para 142.
30 *Ibid* at paras 199–200.
31 See *supra* note 9.

protections of section 8 of the *Charter*. The majority's reasons significantly expanded the scope of section 8 with respect to the types of communications that now attract a reasonable expectation of privacy, as well as the circumstances in which a reasonable expectation of privacy remains in information that has already been communicated.

This massive expansion of the scope of section 8 creates significant difficulties for law enforcement and confusion for courts. In order to give effect to this newly-expanded right while avoiding absurd consequences, courts will be forced to either: (1) water down the current understanding of reasonable and probable grounds in the preparation of search warrant materials; (2) dilute the current tolerance for warrantless searches; or (3) relax the current rules for admission of unconstitutionally-obtained evidence. This watering-down does not exist solely in the third-party text message context: if courts begin to weaken the current protections of section 8 of the *Charter* to avoid absurd policy consequences from the *Marakah* decision, those protections are weakened for all aspects of section 8. The result is that expanding the scope of section 8 for Mr. Marakah weakens its protective strength for all.

Assuming that a reasonable expectation of privacy generally exists where information is communicated in an electronic form to a third party with no legal obligation of confidentiality on the part of a third party — therefore applying to text messages, emails, and other electronic messages — significant practical problems will result. I have identified two factual scenarios that are likely to commonly arise, and I will use these examples to demonstrate the practical problems and impractical solutions that *Marakah* has created. To the extent that these scenarios have been considered in the post-*Marakah* case law, I will outline the approach that courts have tried to take to resolve them.

A. Voluntary Disclosure by the Recipient

First, there is the scenario where the recipient of an electronic communication voluntarily discloses that communication to the police. This commonly occurs in sexual assault or domestic violence cases, where the complainant provides the police with text messages from the accused: for example, where the complainant confronts the accused with an allegation of sexual assault in a text message and the accused responds with

an apology.[32] It is also quite common in charges of uttering threats or criminal harassment, where text messages or written communications from the accused to the complainant constitute the offence.[33] If the recipient of a communication voluntarily discloses that communication to the police, what should the police do?

The majority in *Marakah* declined to answer the question of whether a third party's decision to volunteer a communication to the police affected the sender's reasonable expectation of privacy, though the majority's logic suggests that the sender must still retain a reasonable expectation of privacy in that communication.[34] The majority's decision is premised on the holding that the absence of control over what a third party does with the communication does not mean that there is an absence of a reasonable expectation of privacy in that communication. This assumes that the reasonable expectation of privacy must subsist regardless of what the third party actually does with the information, as the reasonable expectation of privacy exists in the communication itself, not in the written record of that communication on the recipient's device.[35] To conclude otherwise would, in fact, tie the reasonable expectation of privacy to some element of the sender's control over the recipient's device.

This is consistent with the approach that the Supreme Court has taken to other information in the possession of third parties. Thus, for example, an individual does not lose their expectation of privacy in their IP address even where that information is voluntarily provided by the internet service provider to the police.[36] A person whose blood is seized by a medical professional at a hospital does not lose their reasonable expectation of privacy in that blood because the medical professional voluntarily gave the

---

32 See e.g. *R v JFD*, 2017 BCCA 162; *R v Burton*, 2017 NSSC 3 (*Voir Dire* Ruling).

33 Examples of these types of cases are abound. For an example of uttering threats by text message, where the text message was voluntarily provided by the complainant to the police, see *R v Meadus*, 2013 NLTD(G) 108. For an example of a case of criminal harassment by text message, where the messages were voluntarily provided by the complainant to the police, see *R v Wenc*, 2009 ABCA 328 (a sentence appeal but one where the complainant had provided the police with 308 harassing emails and 48 text messages that the accused had sent to her).

34 As the majority suggests that the police ought to obtain a warrant before viewing text messages that are voluntarily disclosed to them. See *Marakah* 2017, *supra* note 1 at para 50.

35 *Ibid* at para 37.

36 *R v Spencer*, 2014 SCC 43 at paras 66–67 [*Spencer*].

blood to the police.[37] The reasonable expectation of privacy, once it is found to exist, can only be ceded by the voluntary actions of privacy-holder[38] or by a lawful search or seizure.[39] Once the reasonable expectation of privacy crystallizes, it can ordinarily only be destroyed by the actions of the privacy-holder or the lawful actions of the state. It is not affected by the actions of private third parties.

One might understandably object to my characterization of the reasonable expectation of privacy that was established by the majority in *Marakah*. After all, the Supreme Court's jurisprudence has generally established that reasonable expectation of privacy is context-specific and determined based on an assessment of the "totality of the circumstances" in any given case.[40] Further, the reasonable expectation of privacy ought to be assessed against state intrusion and determined at the time that the police seek to conduct a search. Just because there was a reasonable expectation of privacy in *Marakah*, where Mr. Winchester did not voluntarily disclose the text messages to the police, does not mean there would be a reasonable expectation of privacy in another case: for example, where the recipient does voluntarily disclose the messages to the police. In every case, the reasonable expectation of privacy must be assessed against the factors recited in *Tessling*, including the place of the search and "whether the information was already in the hands of third parties."[41] This means that, in some cases, there may not be a reasonable expectation of privacy in the contents of one's communications.

While this objection to my characterization is certainly valid, the problem is that this objection is not consistent with the majority's reasoning in *Marakah*. At no point did the majority assess the reasonable expectation of privacy against the state's interest in viewing the messages, nor the legality of the search of Mr. Winchester's phone. It was only after Mr. Marakah's reasonable expectation of privacy was found that the Court went on to consider whether the search of Mr. Winchester's phone was reasonable.[42]

---

37 *R v Dyment*, [1988] 2 SCR 417, 55 DLR (4th) 503 [*Dyment*].

38 See e.g. *R v Patrick*, 2009 SCC 17 [*Patrick*]. The accused had a reasonable expectation of privacy in his garbage but was found to have abandoned that expectation of privacy by placing his garbage in an area accessible to the public (and therefore to the police).

39 *Hunter v Southam Inc*, [1984] 2 SCR 145 at 160–62, 11 DLR (4th) 641.

40 *R v Tessling*, 2004 SCC 67 at paras 31–32 [*Tessling*], citing *R v Edwards*, [1996] 1 SCR 128 at para 45, 132 DLR (4th) 31.

41 *Tessling*, *supra* note 40 at para 32.

42 See *Marakah* 2017, *supra* note 1 at paras 56–57.

In other words, the reasonableness of Mr. Marakah's expectation of privacy was completely divorced from the reasonableness of Mr. Winchester's expectation of privacy in his own phone and messages. The two had no influence on each other. If the majority's reasoning in *Marakah* is faithfully followed, it means that the sender's reasonable expectation of privacy must be assessed before considering the manner in which the police access that information from the recipient. The manner in which that information is accessed has no bearing on whether the reasonable expectation of privacy exists. Instead, it only informs the justifiability of state intrusion on that reasonable expectation of privacy.

If the reasonable expectation of privacy exists in the communication rather than "the contents of a particular cell phone at a particular point in time",[43] it must continue to exist in the communication even if the third party decides to disclose that communication to the state or the world. Consent to a search means the waiver of one's own right to be free from unreasonable search and seizure; a person cannot waive another's right.[44]

To conclude otherwise would, in fact, tie the expectation of privacy to the contents of a particular cell phone at a particular point in time, being the point in time prior to the disclosure of the communication to the police. Otherwise, it would massively expand the scope and meaning of consent in the context of search and seizure by allowing a third party to waive an individual's reasonable expectation of privacy without that individual's knowledge. This then leads to the question that was left relatively unanswered by the majority's reasons in *Marakah*: if the sender of a communication has a reasonable expectation of privacy in that communication regardless of what the recipient does with it, what should the police do with a communication that is voluntarily provided to them?

The cases that considered this issue following the release of *Marakah* but prior to the release of *Mills* were split.[45] Some courts found that that there was no reasonable expectation of privacy in inherently criminal

---

43 *Ibid* at para 37.

44 See Glen Luther, "Consent Search and Reasonable Expectation of Privacy: Twin Barriers to the Reasonable Protection of Privacy in Canada" (2008) 41:1 UBC L Rev 1 at 2.

45 As my thesis is that *Mills* significantly dilutes privacy protections, my interest in examining how courts apply an ostensibly progressive decision in *Marakah* led me to exclude decisions that were released after *Mills* and that can rely on *Mills* for their reasoning.

communications. For example, in *R v Patterson*,[46] the question was whether the accused, who was charged with child luring, had a reasonable expectation of privacy in Facebook messages that he had sent to the victim, who had voluntarily disclosed those messages to the police. The Court found that the accused had no "direct interest" in the messages that he had sent to the victim, as "those messages constitute the *actus reus* of the offence of child luring."[47] It stated that "the constitutional rights which protect our privacy have never gone so far as to permit an accused to claim privacy in respect of his own criminal offences."[48] The Court found that there was no objectively reasonable expectation of privacy in the messages, largely due to the nature of the messages.

At the other end of the spectrum is the British Columbia Provincial Court's decision in *R v Devic*.[49] In that case, the accused exchanged email communications with an anonymous person on Craigslist, who was a member of an organization called "Creep Catchers" and who was posing as an underage female. The Court applied *Marakah*, finding that the accused had a diminished expectation of privacy given that he was conversing with someone that he did not know. The Court further found that the recipient's voluntary disclosure of the messages to the police did not provide the police with lawful authority to seize those messages. The Court stated that "allowing the police to accept the communications from the recipient in the present circumstances would effectively allow the recipient, a third party, to waive the privacy right of the sender in favour of the police", which was inconsistent with *Marakah* and the Supreme Court's decision in *R v Cole*.[50] The Court found a section 8 breach but admitted the messages under section 24(2).[51]

A third example is the British Columbia Supreme Court's decision in *R v Phagura*.[52] In that case, the complainant had attended at the police station and alleged that she had been assaulted by the accused. She showed

---

46 2018 ONSC 4467. It is important to note that this case was decided prior to the Supreme Court's decision in *Mills*.

47 *Ibid* at para 13.

48 *Ibid*.

49 2018 BCPC 318 [*Devic*]. See also *R v Rafferty*, 2018 ONCJ 881, in the context of text messages found on a deceased person's phone which was voluntarily provided to the police.

50 *Devic*, *supra* note 49 at paras 44–45; *R v Cole*, 2012 SCC 53.

51 See *R v Devic*, 2018 BCPC 321.

52 2019 BCSC 1638.

the police text messages on her phone from the accused and the police took photographs of those messages. The Crown sought to introduce them at trial, and the accused relied on *Marakah* in an attempt to exclude them.[53] The Court concluded that the accused lacked an objectively reasonable expectation of privacy in the messages because there was no evidence to show that the complainant similarly expected that the messages would be kept private.[54] In the alternative, the Court reasoned that the police 'search' was authorized by law because it was premised on the consent of the complainant.[55] In other words, the Court suggested that where the police view private information with the consent of the person who received that information, the police have conducted a search that is authorized by law.

On the academic side, Steven Penney has suggested that a search of an electronic conversation can be justified through the third-party consent doctrine. Just as in cases of shared spaces and territorial privacy, the recipient of a communication bears an equal privacy interest in the contents of that electronic conversation. Where the recipient makes an informed and voluntary decision to waive their privacy right in that conversation, this decision ought to be determinative of section 8 issues, even where the accused has made no such waiver.[56] While this is a sensible solution that, if accepted, could erase the privacy paradox altogether,[57] the suggestion of the majority in *Marakah* was that the issue of voluntary disclosure ought to be dealt with through the issuance of a warrant to search the device. I will therefore explore the feasibility of the suggested solution in *Marakah* in order to demonstrate the paradox that *Marakah* created.

B. The Possibility of a Warrant

The majority in *Marakah* suggested that the police could deal with the difficulty of voluntary disclosure of a communication by the recipient by simply obtaining a warrant to view this communication.[58] However, the

---

53 *Ibid* at paras 3–5.

54 *Ibid* at para 51.

55 *Ibid* at para 62.

56 Steven Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap" (2018) 56:1 Alta L Rev 1 at 15–16.

57 However, this solution is inconsistent with the premises of *Marakah*. I discuss this further below in analyzing whether a valid search of the recipient's device constitutes a valid search of the sender's communications.

58 *Marakah* 2017, *supra* note 1 at para 50, "a breach can be avoided if the police obtain a warrant prior to accessing the text messages."

majority provided no guidance on how, exactly, the police could get that warrant; simply saying that it is possible does not make it so. In a scenario where the police would be seeking to obtain a warrant to view a sender's communication on a third party's device, the police would have presumably learned of the existence of the communication in one of four ways: by actually viewing it on the third party's device; by having the third party read the text out to them; by soliciting a screenshot of the text message from the third party; or by relying on a third party's assertion that the text, in fact, exists, but without disclosing its contents. Having learned of this information in one of these ways, the police would have difficulty drafting an adequate Information to Obtain (ITO) that satisfies the current law under section 8 of the *Charter*, leading to both redundancies and absurdities.

First, the police would not be able to rely on the fact that they viewed a text message on the recipient's device in order to obtain a warrant to view that text message. It is well-established that, in assessing whether sufficient grounds exist to obtain a warrant, the police are not entitled to rely on information obtained through an unlawful search or seizure.[59] If there is a reasonable expectation of privacy in a communication in the possession of the recipient, the police would be conducting an unlawful search by viewing that communication in the absence of prior judicial authorization.[60] This means that if the police were to view the text message then attempt to obtain a warrant to seize that text message, the police would be precluded from relying on their knowledge of the contents of that text message when attempting to obtain a warrant to read that text message. If the police cannot rely on their knowledge of the existence of the text message in order to obtain a warrant to view the text message, how can the police satisfy a judge that they have reasonable and probable grounds to believe that a search of the communication would provide relevant evidence?

Perhaps the solution is to have the complainant read the text message out loud or send a screenshot of it to the police, who could then recite it in the ITO and establish the requisite grounds to obtain the warrant to actually view the text message. The police would not have technically "searched" the communication by viewing it directly on the recipient's device, but this seems to be an unduly formalistic understanding of the privacy right

---

59 *R v Grant*, [1993] 3 SCR 223 at 251, [1993] 8 WWR 257 [*Grant*].

60 This was, indeed, the suggestion of the majority in *Marakah* 2017, *supra* note 1 at para 50. The majority suggested that prior judicial authorization was the solution.

recognized in *Marakah*. It would, indeed, be inconsistent with the holding in *Marakah* because it would imply that the privacy right, in fact, inheres in the written record of the communication rather than the communication itself. It would permit the police to rely on an oral account of that communication rather than viewing the written version, thereby implying that the reasonable expectation of privacy only exists in the written version. If the privacy right inheres in the communication itself, the privacy right must subsist regardless of the means by which the recipient might seek to disseminate that communication to others. The police cannot skirt this reasonable expectation of privacy in the communication by asking the complainant to disclose its contents in verbal rather than written form. This would render the privacy right virtually meaningless. Again, this would mean that the police could not rely on their knowledge of the contents of the communication in demonstrating that they have reasonable and probable grounds to believe that the communication affords relevant evidence.

There is one more potential solution: the police could also simply aver that the third party disclosed the existence of a communication in their possession and that they believe that the communication is evidence of an offence (without knowledge of its contents). While this would be permissible, several cautions must be borne in mind. First, the complainant would presumably be required to describe, in some measure of detail, why the communication is relevant evidence of an offence: for example, that it contains a threat, constitutes harassment, contains an apology, provides evidence of timing, or something else. Otherwise the police would be seeking to intrude on a reasonable expectation of privacy with no justification for why such an intrusion is necessary. Section 487 of the *Criminal Code*[61] requires the justice to be satisfied that the place to be searched "will afford evidence with respect to the commission of an offence" before a search warrant may be issued. Similarly, the general warrant provision in section 487.01 of the *Criminal Code* requires the judge to be satisfied that the "information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing" sought to be authorized by the general warrant.[62] Simply asserting that a communication exists without disclosing that communication's relevance to a potential criminal offence may not be sufficient to establish

---

61 RSC 1985, c C-46, s 487(1)(b).

62 *Ibid*, s 487.01(1)(a).

reasonable and probable grounds. There must, therefore, be some level of detail about the contents of the communication.

Where the detail provided by the complainant includes some sort of description of the contents of the communication — for example, where it contains threats — the description of those contents is hearsay for the purpose of the police affiant. The police are circumscribed in their ability to rely on hearsay evidence in an ITO and, depending on the circumstances, hearsay may not be sufficient to establish reasonable and probable grounds.[63]

Further, officers would need to have the foresight to prevent the complainant from showing or reading the communication to them in order to preserve their ability to rely on the hearsay evidence of the complainant in the ITO. This is because the police are required to be full, frank, and honest in an ITO, and the expectance of truthful disclosure is "axiomatic."[64] If the police were to simply aver to the existence of a text message and attempt to rely on hearsay evidence without disclosing the fact that the police had, in fact, viewed that text message, the police would not meet the threshold of full and frank disclosure.[65]

Courts can deal with this issue in one of two ways. First, a court could assess the validity of the ITO in the same manner that it would assess the validity of any other ITO: by excising any information gathered from an unlawful search and then assessing whether the ITO discloses sufficient grounds for the issuance of a warrant.[66] If the affiant referred to the content of the text message in the ITO or the fact that they viewed the text message, this information would be excised and the ITO would likely be insufficient to establish reasonable and probable grounds to obtain a search warrant to view what the police have already viewed. If the affiant did not refer to the content of the text message in the ITO, made full and frank disclosure, and

---

63 *R v Debot*, [1989] 2 SCR 1140 at 1169–70, 37 OAC 1.

64 *R v Szilagyi*, 2018 ONCA 695 at para 59 citing *R v Araujo*, 2000 SCC 65 at para 46 [*Araujo*].

65 See *Araujo*, *supra* note 64 at paras 46–47. The ordinary remedy for a failure to make full and frank disclosure in an ITO is to excise the misleading evidence of the affiant or diminish the reliability of the affiant's information. This may lead to the warrant being quashed as invalid. See e.g. *R v Newman*, 2014 NLCA 48 at para 51; *R v Farrell*, 2013 BCSC 2534 at paras 31–34; *R v Uppal*, 2017 ABQB 373 at para 54.

66 *Grant*, *supra* note 59 at 251-252. This was the approach taken by the Ontario Court of Appeal in *R v Ritchie*, 2018 ONCA 918 at paras 14–17, with respect to ITOs for search warrants for certain financial records and the accused's apartment.

somehow relied on enough hearsay evidence from the complainant to be satisfied of its relevance, a court would be required to assess whether the hearsay evidence, taken alone, is sufficient to establish reasonable and probable grounds. While 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.[67]

Regardless of which route is taken, the outcome is potentially undesirable from a policy perspective. It creates needless and impossible burdens for the police as they seek to obtain prior judicial authorization to view something that they have already viewed or to know something that they already knew. The warrant is both unnecessary and potentially unobtainable. It is unnecessary from a practical perspective because, by and large, the police will have already viewed the text message as a result of the recipient's voluntary disclosure. The requirement for prior judicial authorization to lawfully view what the police have already lawfully[68] viewed seems formalistic, redundant, and virtually impossible: how can one obtain prior authorization to do what has already occurred? The warrant becomes almost unobtainable because, based on the current law applicable to ITOs, the police may be unable to refer to sufficient information about the communication in order to establish that they have reasonable and probable grounds to view that communication. Even if they rely only on hearsay information, they will be found to have failed to make full and frank disclosure if they do not disclose that they have already viewed, i.e. "searched", the communication that they seek to search.

Courts could avoid the undesirable policy outcomes by affirming that an ITO that refers to the contents of a text message or the mere existence of a text message is sufficient to establish reasonable and probable grounds to view that text message. However, this route could have troubling implications. If police are entitled to refer to the content of a text message in seeking judicial authorization to view that text message, an exception to

---

67 See e.g. *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.

68 From the perspective of the complainant's privacy interest, which would have been ceded by voluntary disclosure to the police.

the strong rule set out in *Grant*[69] has been created. For the first time, police would be entitled to refer to information gathered in an unlawful search or seizure to demonstrate that they have reasonable and probable grounds to conduct a search or seizure. While the exception might seem innocuous given the subject matter and the absurdity of the alternative, the fact remains that it would establish the first chink in a long-standing rule protecting against state invasions of privacy. This is troubling.

Courts could also avoid these undesirable policy outcomes by permitting more hearsay evidence in an ITO for a text message search or seizure than would be permitted in other scenarios, given the absurdity of a finding that the police lack reasonable and probable grounds to believe that something they have already viewed contains relevant evidence. Courts may also be more forgiving of the failure to make full and frank disclosure with respect to the reliance on hearsay evidence in this scenario. But if more hearsay evidence is permitted in the text message scenario or if the requirement to make full and frank disclosure is relaxed, the same would presumably apply in other scenarios as well: there is no special warrant for text message searches and seizures,[70] and any judicial rulings on the sufficiency of hearsay evidence in this context apply to other types of searches and seizures authorized by similar warrants. If reliance on hearsay in ITOs becomes more acceptable in order to avoid the absurdities created by *Marakah*, more warrants will presumably be granted. Depending on whether courts confine this increased reliance on hearsay only to the text message context, this has the potential to lead to more warrants being granted based on less reliable evidence, ultimately justifying increased state intrusion on privacy. The crystallization of Mr. Marakah's privacy right may ultimately diminish the privacy rights for all.

C. Lawful Search of the Recipient's Device

The third scenario that is likely to arise is the situation where the police have lawful authority to search the recipient's device — for example, where the police obtain a warrant for that search — but where the police have not

---

69 *Supra* note 59.

70 Unlike the special provisions for things such as production orders and wiretap authorizations, a warrant to search an electronic device and seize communications found on the device is an ordinary warrant under section 487 of the *Criminal Code*. See e.g. *R v Talbot*, 2017 ONCJ 814. The principles that apply to obtaining a warrant to search a cell phone would, therefore, apply to other warrants obtained under that same section of the *Criminal Code*.

obtained prior judicial authorization to search the sender's communications that reside on that device. This scenario would generally arise in areas like organized crime and drug trafficking. For example, imagine a drug trafficking investigation where the police obtain a warrant to search the phone of a street-level trafficker that they have arrested. At the time of the warrant, the police have no knowledge of what is on the trafficker's device; they are simply searching for evidence of drug trafficking. The police search the phone and discover a trove of communications sent from the directing mind of the trafficking operation to the street trafficker. What can the police do with those communications? If they were obtained through an unlawful invasion of the directing mind's privacy rights — even though they were obtained through a lawful search of the street trafficker's device — they may be inadmissible in the eventual trial of the directing mind, even though they would be admissible against the street-level trafficker. As set out above, once the communications are discovered, the police will have difficulty obtaining a warrant to view those communications.

This scenario raises many of the same problems as the voluntary disclosure scenario. Based on the Court's reasoning in *Marakah*, the lawfulness of the search of the recipient's device should have no bearing on the lawfulness of the search of the sender's communication.[71] As a result, the police would end up with the same problem of requiring both an unnecessary and unobtainable warrant to view what they have already lawfully viewed. This is untenable.

It could perhaps be argued that, since the reasonable expectation of privacy inheres in the conversation between the two participants and not the communication from the sender, a valid search of one party's participation in that conversation ought to amount to prior judicial authorization to search that conversation as a whole, and therefore justifies the search of the sender's communication.[72] However, this argument, if accepted, would render the majority's decision in *Marakah* virtually meaningless.

---

71 *Marakah* 2017, *supra* note 1 at paras 56–57. This was framed in terms of a concession by the Crown, but in the context of the *voir dire* judge's ruling that the search of Mr. Winchester's phone was not a valid search incident to arrest.

72 *Ibid* at para 57. This argument could perhaps find its source in the majority's conclusion that "the evidence was obtained by an unreasonable search of the electronic conversation" between the two participants, thereby implying that the evidence is the conversation as a whole rather than Mr. Marakah's communications.

If the reasonable expectation of privacy inheres in the conversation as a whole and the police can validly search and seize it by lawfully searching only one participant's device, the sender's reasonable expectation of privacy becomes tied to the recipient's reasonable expectation of privacy, such that a lawful intrusion on the recipient's expectation of privacy amounts to a lawful intrusion on the sender's expectation of privacy.[73] Even if the sender expected the communications to be private and the police had no suspicion that communications from the sender existed when they obtained a warrant or otherwise lawfully searched the recipient's device, the police would nevertheless be lawfully entitled to seize the communication and the Crown could adduce it as evidence against the sender. This is because a lawful intrusion on the recipient's participation in the conversation would *prima facie* result in a lawful intrusion on the sender's participation in that conversation. This would effectively mean that, if the police had validly searched Mr. Winchester's phone incident to arrest rather than waiting several hours to conduct the search,[74] there would have been no breach of Mr. Marakah's section 8 right.

This argument implicitly equates the justifiability of state intrusion on the recipient's privacy right with the justifiability of state intrusion on the sender's privacy right. It revives the notion of control but transfers it from the reasonable expectation of privacy analysis to the justifiability of state intrusion analysis. Even though the sender's reasonable expectation of privacy is unaffected by the absence of control over the communication on the third party's device, the state would, on this argument, be entitled to intrude on the sender's reasonable expectation of privacy because it has lawful authority to intrude on the recipient's reasonable expectation of privacy. The sender's absence of control over their communications on the recipient's device becomes determinative with respect to the justifiability of the state's intrusion on that reasonable expectation of privacy. If this was indeed the case, the right recognized by the majority in *Marakah* becomes virtually meaningless. For even if an accused has a reasonable expectation of privacy, the permissibility of state intrusion on that reasonable expectation of privacy ultimately depends on the reasonable expectation of

---

73 This was the holding of the British Columbia Court of Appeal in *R v Pelucco*, 2015 BCCA 370 at para 49.

74 *Ibid* at para 65, in the context of the majority's analysis under section 24(2) of the *Charter*.

privacy of the recipient. For all its sound and fury, the majority's judgment would signify nothing.

Prior to the release of *Mills*, these predictions could be validly criticized as speculative or hyperbolic. One could have legitimately argued that courts would not twist, alter, or undermine well-established section 8 principles in order to avoid absurd or undesirable policy consequences. The problem with this argument, however, is that the privacy paradox has been essentially proven by *Mills*. In the Supreme Court's first major digital privacy decision following *Marakah*, a majority of the Court indeed altered and undermined well-established jurisprudence in order to achieve a desired outcome: a finding that an accused person did not have a reasonable expectation of privacy in his online communications with a fictitious child. Once *Mills* is understood as an attempt by the Court to avoid the implications of *Marakah*, the privacy paradox becomes apparent. By expanding the scope of section 8 in *Marakah*, the Court unwittingly set on a path that would undermine section 8 protections for everyone.

IV. The Paradox in Action: *R v Mills*

The Court's 2019 decision in *Mills* concerned an undercover police officer posing on Facebook as "Leann Power", a fourteen-year old girl in St. John's, Newfoundland.[75] "Leann" received a Facebook message from Mr. Mills, who identified himself as being 23 years old. He sent her several messages and emails over the next few months, which included a photograph of his penis as well as the eventual arrangement of a meeting in a public park.[76] When Mr. Mills showed up in the park for the scheduled meeting, he was arrested and charged with one count of child luring. The issues that brought the case to the Supreme Court of Canada were whether the officer ought to have obtained authorization under section 184.2 of the *Criminal Code* to conduct the sting operation, as well as whether the search and seizure of the communications through a screen-grab tool that created a permanent record of them violated section 8 of the *Charter*.[77]

The Supreme Court split four ways in dismissing the appeal and upholding the conviction. Justice Brown, writing for Justices Abella and Gascon, found that Mr. Mills did have a subjective expectation of privacy,

---

75 *Mills*, *supra* note 5 at para 5.

76 *Ibid* at paras 5–7.

77 *Ibid* at para 7.

as he regularly instructed Leann to delete their messages. When she commented on a Facebook post that he had made, he immediately deleted it and then messaged her to say that he did not want his mother to see her comments. Mr. Mills' unsolicited photograph of his penis was accompanied with a warning to "delete this after you look at it!!"[78] The evidence was clear that he subjectively intended that their conversations would remain private.[79]

But Justice Brown found that this subjective expectation of privacy was not objectively reasonable for three principal reasons. First, Mr. Mills was communicating to someone who he believed was a stranger and a child. There is an inherent difference between a relationship involving an adult and an unknown child and other types of relationships, given the inherent vulnerability of children to sexual crimes.[80] Second, this was a situation where the police knew the nature of the relationship between the declarant and the recipient in advance, as the police were posing as the recipient. In his view, the true normative nature of a section 8 privacy interest is not in the thing searched or seized, but in the nature of the relationship between the parties subjected to state surveillance.[81]

Third, he found that the subjective expectation of privacy was objectively unreasonable because of the nature of the investigative technique used. The police knew from the outset that the accused's relationship with the child was fictitious and, therefore, that no section 8 concerns would arise from them reviewing the accused's communications with that child.[82] Unlike *Marakah*, the police were not intruding on an established relationship between two persons. In this case, they created and controlled the relationship.[83] He also found that this distinguished it from the situation in *Duarte*, where the police surreptitiously recorded a conversation between an undercover informer and the accused.[84] He,

---

78 *Ibid* at para 18.

79 *Ibid*.

80 *Ibid* at paras 22–23.

81 *Ibid* at paras 25–26. How he reconciles this with non-relationship-based cases such as *Patrick*, *supra* note 38 and *Tessling*, *supra* note 40 remains unexplained.

82 *Ibid* at para 27.

83 *Ibid*.

84 *Ibid* at para 28. He did not explain why this situation was distinguishable from *Duarte* other than to conclusively say that it was so. Presumably, he meant that the creation of a permanent electronic record of the communication through the use of the screen grab tool was different from the recording of a conversation between an accused and an undercover officer or police informer.

therefore, concluded that there was no reasonable expectation of privacy, no section 8 breach, and, because no "private communication[s]" were intercepted, no breach of section 184.2 of the *Criminal Code*.[85]

Justice Karakatsanis, writing for herself and Chief Justice Wagner, reached the same conclusion through a different route. In her view, there was no search or seizure and, therefore, section 8 of the *Charter* was not engaged at all. She relied on statements from *Duarte*, distinguishing conversations between undercover officers and accused persons from the recording of those conversations, stating that no search or seizure occurs where an accused person unwittingly chooses to speak to an undercover officer.[86] She found no distinction between a verbal conversation and a written one, stating that section 8 also would not be triggered if an accused unwittingly wrote a letter or passed a note to an undercover officer.[87] No authority was cited for this proposition. She distinguished this from the situation in *Duarte*, as the person speaking to an undercover officer has no knowledge that they are being recorded. In the case of electronic communications, the "speaker" knows that they are being recorded because the speaker is intentionally creating that record.[88]

Justice Karakatsanis further held that the use of the screen grab tool to create screenshots of the electronic communications did not amount to a search or seizure. She found no reasonable difference between the state preserving the communications by using a screen grab tool, tendering the screenshots into evidence and simply tendering a laptop or phone with the communications open into evidence.[89] She tempered the implications of

---

85 *Ibid* at paras 32–34.

86 *Ibid* at paras 42–43; *R v Duarte*, [1990] 1 SCR 30, 65 DLR (4th) 240 [*Duarte*].

87 *Mills*, *supra* note 5 at para 45.

88 *Ibid* at para 48.

89 *Ibid* at para 56. How the latter approach could be reconciled with the Crown's disclosure obligations is unclear, given that the Crown cannot disclose to the defence an open laptop or cell phone. Perhaps defence counsel could attend the police station and simply view the conversation on the laptop or cell phone (as occurs in some jurisdictions with sensitive child pornography materials), but without touching or altering the conversation to preserve continuity. Perhaps, since there is no prohibition on the disclosure of unconstitutionally-obtained evidence, the Crown could disclose the screenshots to the defence but tender the evidence on the laptop; thereby potentially infringing section 8 by taking a screenshot and formalistically avoiding the effect of that infringement by tendering the laptop instead of the screenshot. The point being that legitimizing the polices' ability to take and adduce screenshots by analogy to a practice

her conclusion by stating that this does not mean that undercover, online police operations will never intrude on a reasonable expectation of privacy, given technological advancements.[90]

Justice Moldaver, writing alone, stated that he concurred with the reasons of both Justices Brown and Karakatsanis and would dismiss the appeal.[91]

Finally, Justice Martin, writing alone, would have dismissed the appeal but on different grounds. She accepted that Mr. Mills had an objectively reasonable expectation of privacy in his online communications. Justice Martin saw no normative difference between *Duarte* — decided at a time where the only technological possibility for creating a record of a conversation was to record a verbal conversation — and the facts of *Mills*. Both situations involved state access to the electronic record of a conversation. The fact that the participant in an electronic communication knows that there is an electronic record of the conversation is not determinative, as the expectation of privacy is not about the record itself but rather about the possibility of state access to that record.[92]

Justice Martin saw no determinative significance to the fact that the declarant creates the permanent record themselves when communicating through electronic means. This is because "awareness that one's conversation is documented does not necessarily negate the objective reasonableness of the expectation that the state will not access that documentation."[93] However, she acknowledged that the significance of this element can shift depending on the type of communication at issue: for example, letters and notes rather than spontaneous electronic conversations.[94]

Justice Martin then critiqued many of the premises and conclusions in the reasons of Justices Brown and Karakatsanis. She challenged Justice Karakatsanis' reliance on the analogy between verbal conversations and electronic conversations with undercover officers, noting that the possibility for mass surveillance exists in the electronic sphere in a way that it cannot exist in the real world. Further, the anonymity afforded by the internet

---

that is not currently done is unwieldly, potentially impossible, and not a particularly convincing point.

90 *Ibid* at para 57.

91 *Ibid* at paras 66–67.

92 *Ibid* at paras 90–91.

93 *Ibid* at para 97.

94 *Ibid* at para 102.

enables the police to create numerous, richly textured, and believable false identities in order to conduct as much surveillance as they wish. This is a possibility that simply does not exist in the context of actual undercover officers performing physical operations, and the analogy to undercover participants in verbal conversations is therefore flawed.

She then critiqued the conclusions of Justice Brown regarding the impact of the nature of the relationship and the content of the communications on the objective reasonableness of an expectation of privacy. Justice Martin viewed the new criterion of the nature of the relationship as a proxy for the rejected concept of "control", based on a risk analysis that has been repeatedly rejected in the Supreme Court's prior section 8 jurisprudence.[95] Further, the fact that the individual is engaged in illegal activity ought to be irrelevant to the section 8 analysis, as the Court has repeatedly state that section 8 is content-neutral and unconcerned with whether it is sheltering legal or illegal behaviour.[96] She found no legitimate reason to exclude relationships between adults and children from the section 8 analysis, noting that section 8 has been found to protect activities of adults in the context of digital or internet-based sexual crimes involving children.[97]

Justice Martin ultimately concluded by finding that it is objectively reasonable for members of society to expect that the state will only access recordings of their private conversations — electronic or otherwise — with judicial authorization. She therefore found a section 8 breach but would have admitted the evidence under section 24(2).[98]

V. Proving the Paradox

Understanding *Mills* as an example of the privacy paradox in action requires one to attempt to reconcile *Mills* and *Marakah*. This is no easy task. Outside of Justice Martin's opinion in *Mills*, the two decisions are like ships passing in the night. Indeed, it appeared that Justice Brown's majority decision in *Mills* attempted to grapple with the implications of *Marakah* by, essentially, ignoring it completely. For example, Justice Brown dismissed the claim that Mr. Mills had an objectively reasonable expectation of privacy in

---

95 *Ibid* at para 110.
96 *Ibid* at para 118.
97 *Ibid* at para 120.
98 *Ibid* at paras 133, 149–55.

the messages without even applying the test for assessing the objective reasonableness of an expectation of privacy.[99] The test for assessing the objective reasonableness of an expectation of privacy in electronic communications, as affirmed in *Marakah*, involves the assessment of four factors: the place of the search; the private nature of the information; control; and other policy considerations.[100] Justice Brown appeared to skip the first three factors and jump straight to policy considerations, concluding that it is not objectively reasonable for adults to expect privacy in their online conversations with children who are strangers to them.

The majority in *Marakah* held that the possibility of police interception cannot be considered when determining a reasonable expectation of privacy.[101] For the majority in *Mills*, this possibility of police "interception" through police participation in the conversation was, in fact, determinative of the reasonableness of Mr. Mills' expectation of privacy. This is because, though Mr. Mills was unaware that he was conversing with a police officer, the police knew that he was conversing with a police officer.[102] The fact that the police were always aware that Mr. Mills was not communicating with an actual child was determinative of the objective reasonableness of his expectation of privacy. In effect, it was <u>because</u> the messages were directly "intercepted" by the police that Mr. Mills could not reasonably expect that the messages would be kept private from the state.

The Court's decision in *Marakah* recognized that a person who engages in electronic conversations may reveal details about their activities, relationships, and identities that they would never reveal to the world at large, while expecting privacy in doing so.[103] Control over electronic communications is exercised when one determines for oneself "when, how, and to what extent information about them is communicated to others",[104] regardless of who those others might be. For the majority in *Mills*, the

---

99 Justice Brown did not assess any of these factors in the context of the objective reasonableness of the expectation of privacy, instead focusing only on the nature of the relationship between Mr. Mills and the recipient and the particular investigative technique used. He did not mention the place of the search, the private nature of the information, or control in his assessment of the objective reasonableness of Mr. Mills' expectation of privacy.

100 *Marakah* 2017, *supra* note 1 at para 24.

101 *Ibid* at para 34.

102 *Mills*, *supra* note 5 at paras 24, 27, 29, 44–45, 48, 50–52.

103 *Marakah* 2017, *supra* note 1 at para 36.

104 *Ibid* at para 39, quoting Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1970) at 7.

identity of the "other" was determinative, as the accused could not reasonably expect privacy when he bore the risk of communicating with a stranger,[105] especially when he believed that stranger was a child. The content of Mr. Mills' messages and his expressed desire for privacy appeared irrelevant to the majority's assessment of the objective reasonableness of his expectation of privacy. While the Court in *Marakah* assessed the reasonable expectation of privacy from the perspective of the accused, the majority in *Mills* assessed that expectation from the perspective of the police.

While this is not a case comment on *Mills*, my argument that the majority's reasons are an example of the privacy paradox in action requires some elaboration on why I view the majority's reasoning as an erroneous departure from the Court's prior case law. This is because the paradox is premised on the assumption that courts would ignore or water down well-established principles under section 8 in order to avoid absurdities flowing from the conclusion in *Marakah*. It is thus necessary to analyze the errors in the majority's reasons to establish this premise.

With respect to Justice Brown's reasons, he did not apply the well-established factors from *Tessling*, *Patrick*, and *Marakah* with respect to the assessment of an objectively reasonable expectation of privacy. In *Tessling*, Justice Binnie directed judges to assess a variety of factors to determine whether an asserted expectation of privacy was objectively reasonable, including the place of the search; the subject matter of the search and whether it was in public view or had been abandoned; whether the information was already in the hands of third parties; the intrusiveness of the police technique in relation to the privacy interest; whether the use of surveillance technology was itself objectively unreasonable; and whether the police technique used exposed any intimate details of the person's lifestyle or information of a biographical nature.[106] Subsequent cases expanded on each of these elements.

In *Mills*, Justice Brown did not assess the place of the search, though this failure might be justified based on the incompatibility of a place-based approach to privacy with digital privacy.[107] He did not assess whether the information was in "public view", i.e. available for the world to see, or

---

105 *Marakah* 2017, *supra* note 1 at paras 23–24.

106 *Tessling*, *supra* note 40 at para 32.

107 *Marakah* 2017, *supra* note 1 at para 28; Stern, *supra* note 6 at 408–12.

whether Mr. Mills attempted or intended to keep it private.[108] Justice Brown also did not assess the private nature of the information nor the potential for Facebook messages and emails to reveal private information. He made no mention of control, although he implicitly found that the absence of control weighed in favour of no section 8 breach, a point that directly conflicts with *Marakah*.[109] In Justice Brown's view, the state's intrusion on Mr. Mills' private conversations was justified because those conversations were not, in reality, private. Instead, Mr. Mills was unwittingly conversing with an agent of the state through a medium that he believed to be private. The fact that he had no confirmation of the identity of the recipient and, therefore, implicitly had no control over what that recipient chose to do with his messages negated the objective reasonableness of his expectation of privacy.

With respect to what should have been assessed in the last three *Tessling* factors, Justice Brown's reasoning becomes rather circular. In essence, he found that Mr. Mills had no reasonable expectation of privacy because of the intrusiveness of the police technique: by duping Mr. Mills into revealing profoundly personal details in a conversation that he believed, expected, and requested to be kept private, any objective reasonableness of Mr. Mills' expectation of privacy was erased.[110] Had the police adopted a less intrusive method to collect evidence of sexual crimes against children — for example, by requesting copies of messages from Facebook that the police believed to contain inappropriate sexual contact between adults and children — the declarants would almost surely have an objectively reasonable expectation of privacy.[111] But because the state was directly involved in the creation of the messages — regardless of whether the author of the messages knew that — the declarant lacked a reasonable expectation of privacy. In effect, the

---

108 This fact was only mentioned in the context of Mr. Mills' subjective expectation of privacy. See *Mills*, *supra* note 5 at paras 18–19.

109 *Mills*, *supra* note 5 at para 22.

110 The legality of this tactic in future digital privacy cases may be questionable in light of the Supreme Court's recent decision in *R v Ahmad*, 2020 SCC 11 [*Ahmad*], which provided some tools for adapting the law of entrapment for the digital age. A majority of the Court held that the police must have reasonable suspicion that a particular target is engaged in criminal activity or that criminal activity is occurring in a particular place before the police may provide someone with the opportunity to commit a crime in the targeted place. While *Ahmad* was a dial-a-dope case, it may have a significant effect on future *Mills*-type investigative techniques.

111 *R v Jones*, 2017 SCC 60 at para 45 [*Jones*].

majority in *Mills* held that the intrusiveness of the police technique destroyed the reasonable expectation of privacy, rather than defining it.

Justice Brown appeared to anchor his reasoning on the concept of a "relationship-based" approach to privacy, sourcing it in the Supreme Court's decision in *Dyment*.[112] He began by treating this relationship-based understanding as, essentially, a proxy for control. Where information or potential evidence is in the hands of a third party, a reasonable expectation of privacy may nevertheless remain depending on the nature of the relationship between the source of the information and the third party. Thus, a doctor is expected to keep a patient's bodily samples private;[113] an internet service provider is statutorily and/or contractually obliged to keep subscriber information private;[114] and a cell phone provider is required to keep stored text messages private.[115] However, instead of using the nature of the relationship as a proxy for control over the particular information that is being protected by section 8, Justice Brown treated the relationship itself as the object of section 8's protection.[116] Instead of protecting information or core biographical data from state intrusion, section 8 now protects particular relationships from state intrusion.

While Justice Brown appears to suggest that the *Dyment* decision supports his approach,[117] this conflates informational privacy with the concept of control. The two are not the same. In *Dyment*, the accused had a reasonable expectation of informational privacy in his blood. While he implicitly consented to the drawing and use of this blood for medical purposes, he did not consent to its use by the police in a criminal prosecution.[118] The fact that it was taken from his body and in the hands of a physician did not destroy this informational privacy; the accused's residual control through his relationship with his physician ensured that his expectation of privacy remained. But the privacy interest was in the blood itself, not in the relationship between the accused and his physician.[119]

---

112 *Mills*, *supra* note 5 at paras 25–26; *Dyment*, *supra* note 37.

113 *Dyment*, *supra* note 37 at 418.

114 *Spencer*, *supra* note 36 at paras 65–66.

115 *Jones*, *supra* note 111.

116 *Mills*, *supra* note 5 at para 26.

117 *Ibid* at para 25 [emphasis in original], "[t]he s. 8 interest was not viewed by the Court as being concerned solely with *the blood*, but principally with the relationship between the patient and the physician."

118 *Dyment*, *supra* note 37 at 431–32.

119 *Ibid* at 432.

Justice Brown's revision of *Dyment* to create a relationship-based understanding of section 8 is remarkable. It places courts in the business of assessing relationships in which information is gathered and ultimately disclosed to the state in order to determine whether that particular relationship is one worthy of *Charter* protection. The information itself and its importance to the person who is claiming privacy in it is largely irrelevant. Consider how this would apply to a situation like *R v Stillman*:[120] if the privacy interest is in the relationship and not the information, then an accused person who is in lawful police custody has no reasonable expectation of privacy in bodily samples that are seized from him by the police. An officer could directly draw blood from the accused without judicial authorization and use the informational contents of that blood as evidence against the accused, without the accused being able to claim the protection of section 8 of the *Charter*.

While Justice Brown might understandably protest this articulation of the implications of his conclusion,[121] such a protest would presumably be premised on the argument that there is a difference between a relationship-based understanding of privacy between private individuals and the privacy interest that one holds directly against the state. In the former, section 8 protects the relationship itself, while in the latter, section 8 protects the intimate details of a person's life, such as those disclosed by bodily samples, against unauthorized state intrusion. But to uphold this protest would be to undermine Justice Brown's reasoning in *Mills*, as Justice Brown denied the latter concept of informational privacy in a direct relationship between the accused and the state. By concluding that the relationship itself was not worthy of protection, he concluded that there was no reasonable expectation of privacy in the information that the accused believed he was privately disclosing.

Without *Marakah* and its diminishment of the element of control in the objective expectation of privacy analysis, it is likely that Justice Brown would have reached the same conclusion that Mr. Mills had no objectively reasonable expectation of privacy without undermining decades of *Charter* law. If control was still the predominant factor to be considered, the Court

---

120 [1997] 1 SCR 607, 144 DLR (4th) 193. For those unfamiliar with *Stillman*, it involved the police forcibly taking hair samples and teeth impressions from the 17-year-old accused while he was in police custody and subject to intense interrogation.

121 As he did to similar suggestions made by Justice Martin in her dissent. See *Mills*, *supra* note 5 at para 30.

would have easily concluded that Mr. Mills lacked an objectively reasonable expectation of privacy in messages that were found on the recipient's device, regardless of whether that recipient was a police officer or an actual child. Mr. Mills simply had no control over what the recipient chose to do with his messages, as he could only hope that the recipient would agree to keep the messages private and delete them regularly.[122] A hope is not the same as a reasonable expectation of privacy, especially when the stranger is not personally known to the accused. An accused simply has no control over information in the hands of third parties in the absence of a legal requirement to keep that information confidential. An accused, therefore, has no reasonable expectation of privacy in that information. However, given the majority holding in *Marakah*, this line of reasoning was not open to the Court in *Mills*.

Justice Brown concluded that there were no broader implications of his decision because it was confined to the narrow facts of this case.[123] But, saying it is so does not make it so. By declining to engage with *Marakah* and sidestepping its implications, the majority's reasons in *Mills* have taken Canadian privacy law in a significant backward direction. The implications of *Mills* are chilling. A person engaging in text, email, or online communications must self-censor on the possibility that the recipient is an agent of the state, as the declarant cannot speak freely with the knowledge that a permanent record of his words can and will be used as evidence against him. This is because police tactics aimed at manipulating a person's expectation of privacy in online communications to create evidence of an offence are now recognized as permissible, even without judicial authorization.[124] A person engages in online communications precisely because they expect them to be private. After all, "there is no more discreet form of correspondence" than text messaging or other types of electronic communications.[125]

It is no answer to say that a person can still engage freely in online conversation with persons whose identity is known to that individual. Such an argument is based on a false analogy to face-to-face conversations which denies the realities of the online world and creates an impossibly blurred standard. There is a significant difference between speaking to a person face-

---

122 *Ibid* at para 19.

123 *Ibid* at para 30.

124 Subject to the jurisprudence that may develop after *Ahmad*, *supra* note 110.

125 *Marakah* 2017, *supra* note 1 at para 35.

to-face, where the speaker can generally verify the identity of the other participant in the conversation and speaking to an individual online. A person who is engaging in digital conversations may not be who they say they are; even if an individual believes they are conversing with a person who is known to them, they may, in fact, be conversing with someone completely different, including a police officer. As Justice Martin pointed out in her dissent in *Mills*, it is all too easy to impersonate another online.[126] This is true whether one creates an entirely false identity, as the police did in *Mills*, or where one impersonates another that is known to the individual. The implication of *Mills* is that it is a risk inherent to all online conversations that the recipient may not be who they say they are and that because of that risk, an individual therefore has no reasonable expectation of privacy in the contents of their communications.

One might answer this argument by pointing to *Duarte*: just as a person must assume the risk that the individual to whom they are speaking face-to-face is an agent of the state, a person engaged in online or electronic communications must assume the risk that the recipient of their communications is not the person whom they believe it to be. This was, indeed, the basis of Justice Karakatsanis' separate opinion in *Mills*.[127] But this takes *Duarte* too far: *Duarte*'s holding was premised on the difference between a verbal conversation and a record of that conversation.[128] While a person must always assume the risk that the recipient of their communications will disclose those communications, the *Charter* protects against "the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words."[129] The normative rationale for this protection is that, absent it, "there would be no meaningful residuum to our right to live our lives free from surveillance."[130] While *Duarte* was decided before the age of electronic communications, there would be some irony in using its principled protection of privacy to undermine privacy rights because participation in society has become increasingly electronic. As Justice Karakatsanis noted in *R v KRJ*, "[f]or many Canadians, membership in online communities is an integral component

---

126 *Mills*, *supra* note 5 at para 106.
127 *Ibid* at paras 48–50.
128 *Duarte*, *supra* note 86.
129 *Ibid* at para 23.
130 *Ibid* at para 24.

of citizenship and personhood."[131] The internet is, in many respects, the new public space where relationships are fostered, business is conducted, and people live all aspects of their lives.[132] To deny an individual privacy against the state where such privacy would have been granted had the same conversation occurred face-to-face would severely diminish the adaptability of section 8 to the digital age.

To return to the premise of this article: would we have *Mills* without the well-meaning but ultimately flawed decision in *Marakah*? In my view, we would not. This is because without *Marakah*, the element of control would have been determinative in *Mills*. The Court would have easily found that Mr. Mills had no control over his communications once they were sent and therefore ceased to have a reasonable expectation of privacy in them. Indeed, this was the precise reasoning of the Newfoundland Court of Appeal in *Mills*, which released its decision without the benefit of the Supreme Court's reasons in *Marakah*.[133] Without *Marakah*, there would have been no need to alter the course of section 8 of the *Charter* to achieve what all judges of the Supreme Court saw to be a just result: the use of Mr. Mills' communications with "Leann" to convict him of child luring offences.

But what about the facts in *Marakah*, one might ask? Surely the police should not be able to skirt the well-established requirement to obtain prior judicial authorization to access one party's text messages simply by conducting an unconstitutional search of the recipient's phone. I agree that the police should not be able to do so, but in a perfect world, *Marakah* ought not to have been a section 8 case at all. If the mischief was that the police were deliberately manipulating and avoiding well-established legal rules to ensure that evidence would be admitted at trial, that action ought to be treated as an abuse of process under section 7. But this is not a perfect world, and the doctrine of abuse of process under section 7 has been severely limited by the courts. As *Marakah* has shown, it is easier to obtain a novel ruling significantly expanding section 8 of the *Charter* than it is to obtain a narrow remedy for abuse of process.[134] But, this is a problem for

---

131 *R v KRJ*, 2016 SCC 31 at para 54.

132 *Ibid*, citing Bradley Areheard and Michael Stein, "Integrating the Internet" (2015) 83 Geo Wash L Rev 449 at 456.

133 *R v Mills*, 2017 NLCA 12 at para 23.

134 *Marakah* 2017, *supra* note 1 at para 192. Justice Moldaver alluded to this state of affairs in his dissent, where he noted that deliberate *Charter* evasion by the police "can be fully addressed under ss. 7 and 11(d) of the *Charter*."

another day. The point is simply that the remedy in *Marakah* — exclusion of the evidence — could have been obtained without necessarily expanding the scope of section 8 and creating the paradox that led to *Mills*, which may ultimately restrict the protections of section 8 for all.

VI. Conclusion

This article is about how well-meaning judicial decisions can have unintended results. The Court in *Marakah* intended to narrowly expand section 8 of the *Charter* to ensure that the police could not avoid their obligation to obtain prior judicial authorization simply by obtaining the accused's text messages from the recipient's device. This expansion, however, was anything but narrow. As a result, the Court tried to rein in the expansion in *Mills* to avoid the undesirable result of the *Charter* shielding an accused's attempts at child luring from prosecution. The net result is a confusing mess of section 8 of the *Charter*: it protects communications that are intended to be kept private but not those communications that are intended to be kept private and end up being directly received by the police. It encourages the police to prey on citizens' expectations of privacy online without any judicial oversight whatsoever; as long as the police are able to create a sufficiently real dupe, the accused's subjective expectation of privacy becomes objectively unreasonable. While *Marakah* sought to ensure that citizens could communicate as freely online and in digital formats as they can verbally, *Mills* erased that assurance. Online and digital communications must be self-censored unless the accused knows the recipient, as the accused must otherwise expect that these communications can and will be used against them. And even if the accused knows the recipient, courts are now in the business of determining whether the relationship between the accused and the recipient, as well as the contents of their communications, are worthy of constitutional protection.[135]

Mills fulfills the privacy paradox. In an attempt to address the unintended consequences of *Marakah*, the Court significantly reduced the protections of section 8 of the *Charter* in the digital age. Expanding section 8 in *Marakah* arguably led to the overall dilution of section 8 in *Mills*. These

---

[135] See e.g. *Heppner*, *supra* note 9 at para 58, concluding that the accused's email communications to the complainant were not protected by section 8 because the complainant was a vulnerable person.

two cases present a cautionary tale about *Charter* decisions that are lauded as progressive: unintended implications may undermine and ultimately negate any progressive gains made by that decision. Courts, therefore, ought to think carefully about the practical and legal paradoxes that progressive decisions can create. While it may be unpopular to decide a case like *Marakah* narrowly or to grant a fact-based remedy like a remedy for abuse of process,[136] this may ultimately lead to more progressive developments of the protections of the *Charter* in the long run.

[136] Which would arguably require a less-restrictive understanding of abuse of process in section 7. I recognize the irony of suggesting this as an alternative to expanding the scope of section 8 to grant the remedy sought. But the point here is that a finding of abuse of process is generally fact-specific and does not require the Court to establish any new legal principles.