Talking to Strangers: A Critical Analysis of the Supreme Court of Canada's Decision in *R v Mills*

CHELSEY BUGGIE*

ABSTRACT

In *R v Mills*, an undercover officer acting without a warrant posed as a 14-year-old girl online and communicated with Mr. Mills through Facebook messages. The officer eventually arranged a meeting with, and arrested Mr. Mills who sought to have the message evidence excluded.

The Supreme Court unanimously ruled to allow the evidence. However, only Justice Martin agreed that Mr. Mills' s. 8 rights were engaged and infringed. This paper takes the position that the *Mills* decision is inconsistent with prior s. 8 jurisprudence regarding content neutrality and expectation of privacy in conversations. The type of sting operation used in *Mills* should have been classified as participant surveillance requiring a warrant.

In *Mills*, the Supreme Court unduly adjusted the balance of power to favour law enforcement. The result of the *Mills* decision is that law enforcement may continue to use this investigative technique unregulated, and unencumbered. Such an adjustment in favour of law-enforcement is not justified. Other investigative techniques are available to law enforcement and obtaining a warrant would not unduly hinder child luring investigations. Failure to oversee these operations could have a potential

* Chelsey Buggie recently obtained her Juris Doctor from the University of New Brunswick's Faculty of Law and is currently pursuing a Masters of Technology Management at Memorial University. Chelsey has a strong interest in privacy law, as well as the intersections of novel technologies and criminal law. The author is grateful to the three anonymous reviewers of this paper for their helpful comments. She would also like to extend her gratitude to Dr. Kerri Froc for her extensive feedback and support.

chilling effect on legitimate online relationships and reinforce stereotypes about hypersexualized youth online.

Keywords: Child Luring; Section 8; Search and Seizure; Participant Surveillance; the *Duarte* Principle

I. INTRODUCTION

In 1982, Compaq introduced the first "portable" computer. It was the size of a sewing machine and weighed 28 pounds. 1982 is also the year that the *Canadian Charter of Rights and Freedoms* came into force. S. 8 of the *Charter* guarantees that "[e]veryone has the right to be secure against unreasonable search or seizure."[1] Its purpose is to prevent unjustified searches from occurring, which can only be accomplished "by a system of prior authorization, not one of subsequent validation."[2] In *Hunter v Southam Inc*, the Supreme Court of Canada unanimously explained that s. 8 "must… be capable of growth and development over time to meet new social, political and historical realities often unimagined by its framers."[3] For example, in 1982, it would be difficult to imagine that Canadians would one day hold computing power in the palm of their hand and carry years' worth of written correspondence in their pockets.[4]

In 1997, just 22% of Canadian households owned one cellphone for personal use; by 2019, 89% of internet-users owned a smart-phone.[5] With the advancement of technology comes new methods of committing crimes. In the not-so-distant past, purchasing an illegal firearm likely involved meeting a stranger in a potentially unsafe location. Today, the same firearm can be purchased anonymously through the darknet using an untraceable cryptocurrency and be delivered directly to the buyer's doorstep. Law enforcement lament that the advancement of technology has outpaced their ability to solve crimes, calling on legislators and judges to "restore the pre-

---

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

2 *Hunter v Southam Inc*, [1984] 2 SCR 145 at 160, 11 DLR (4th) 641 [*Southam Inc*] [emphasis in original].

3 *Ibid* at 155.

4 Gerald Chan, "Text Message Privacy: Who Else is Reading This?" (2019) 88 SCLR Osgoodes Constitutional Cases Conference at 74 [Chan, "Text Message Privacy"].

5 *R v Canfield*, 2020 ABCA 383 at para 28 [*Canfield*].

digital status quo."[6] Equilibrium adjustment theory suggests that when changing technology expands police power, courts can tighten constitutional privacy protections to restrict police power and restore the status quo; conversely, when police power is overly restricted, courts can loosen protections to achieve the same goal.[7]

In the 2019 case of *R v Mills*,[8] an officer acting without prior judicial authorization (a warrant) posed online as a 14-year-old girl and engaged in conversations with Mr. Mills through Facebook Messenger and Hotmail, taking screenshots of the conversations. The officer also connected with other minors online to make the profile appear legitimate.[9] Eventually, the officer arranged a meeting where Mr. Mills was subsequently arrested and charged with child luring. Mr. Mills argued that he had a reasonable expectation of privacy in the conversation under s. 8 of the *Charter* and that the screen-shot evidence should be excluded. The Supreme Court allowed the screen-shot evidence to be admitted.

This paper will provide a critical analysis of the Supreme Court of Canada's decision in *R v Mills*, arguing that the decision is inconsistent with prior s. 8 jurisprudence and unduly shifts the balance of power to favour law enforcement. This paper reviews the s. 8 jurisprudence leading up to *Mills* on matters such as participant surveillance and the expectation of privacy in electronic conversations. Prior to *Mills*, the s. 8 analysis proceeded in a content-neutral manner. This paper takes the position that the *Mills* decision contradicts prior s. 8 jurisprudence in particular *Duarte* and *Marakah*. The decision creates ambiguity as to who constitutes a "stranger". This ambiguity, along with policing marginalized sexual communities could have the effect of chilling legitimate online communications. Finally, this paper will address why such a shift in the balance of power is unwarranted and argue that these operations should be subject to regulation.

Despite the fact that cellphones have been widely used for over a decade, the first cases addressing text-message privacy under s. 8 of the *Charter* did not reach the Supreme Court of Canada until the case of *R v*

---

6 Steven Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014) 67 SCLR Osgoodes Constitutional Cases Conference at 505 [Penney, "Digitalization of Section 8"].

7 Owen S. Kerr, "An Equilibrium Adjustment Theory of the Fourth Amendment" (2011) 125 Harvard LR at 482.

8 *R v Mills*, 2019 SCC 22 [*Mills*].

9 Tamir Israel Samuelson-Glushko, *Digital Privacy in Emerging Contexts* (Canadian Internet Policy & Public Interest Clinic, 2019) at 11.

Marakah and its companion case *R v Jones* in 2017.[10] Both Marakah and Jones were accused of trafficking firearms and law-enforcement wished to obtain copies of their text-messages from consenting third parties without prior judicial authorization. In *Marakah*, a majority of the Supreme Court recognized that a reasonable expectation of privacy exists in a conversation, even after the message is no longer in the sender's control.[11] In *Jones*, the Supreme Court held that police require a production order to obtain copies of text messages from a service provider.[12] Chief Justice McLachlin (as she then was) wrote: "In consequence, the fruits of a search cannot be used to justify an unreasonable privacy violation. To be meaningful, the s. 8 analysis must be content neutral."[13]

Although the *Mills* decision is technically a unanimous decision as to the admissibility of the text-message evidence, it is anything but unanimous with respect to the principles in the case. Justice Brown, writing for a "pseudo-majority" of himself, Justices Abella and Gascon concluded that there is no expectation of privacy in messages sent to children who are strangers, therefore s. 8 was not engaged.[14] In a concurring judgement, Justice Karakatsanis with Chief Justice Wagner concurring determined that no search or seizure occurred as the undercover officer was the intended recipient. She writes that individuals cannot expect that their messages will be kept private from the person with whom they are communicating.[15] Justice Moldaver concurs with both assertions, writing "each set of reasons is sound in law."[16] Justice Martin found that the accused had a reasonable expectation of privacy in the messages, and that his s. 8 rights were infringed, but excluding the message evidence would bring the administration of justice into disrepute.[17] Such a divide in reasoning will almost certainly lead to confusion as to how lower courts should apply the law.[18]

---

10 Chan, "Text Message Privacy", *supra* note 4 at 69.
11 *R v Marakah*, 2017 SCC 59 [*Marakah*].
12 *R v Jones*, 2017 SCC 60 [*Jones*].
13 *Marakah*, *supra* note 11 at para 48.
14 *Mills*, *supra* note 8 at paras 27–29.
15 *Ibid* at paras 36–37.
16 *Ibid* at paras 66–68.
17 *Ibid* at paras 72–73.
18 Peter McCormick, "When Judicial Disagreement Doesn't Matter" (15 November 2018), online: *Double Aspect* <doubleaspect.blog/2018/11/15/when-judicial-disagreem

The decision of Justice Martin is arguably most consistent with prior s. 8 jurisprudence. The Supreme Court has routinely taken a firm stance against warrantless electronic police surveillance even where the target of said surveillance is participating in illegal activity. In *Wong*, the Supreme Court found that a person had an expectation that they would be free from police surveillance in a hotel room, even while hosting an illegal gambling event.[19] Later, in *Duarte*, the Court determined that police could not use a video camera to observe an undercover officer communicating with the accused without prior judicial authorization.[20]

In *Mills*, the Court abandons content-neutrality and considers the nature of the crime in the s. 8 analysis. Justice Martin asserts that this "put[s] courts in the business of evaluating the Canadian public's personal relationships with a view to deciding which among them deserve *Charter* protection under s. 8."[21] Ambiguity as to who constitutes a "stranger" could have a potential chilling effect on legitimate online communications.[22] The result of the *Mills* decision is that law enforcement may continue to use this sting technique unregulated, and unencumbered.[23]

II. SECTION 8 JURISPRUDENCE

A. Framework for Evaluating Claims Under Section 8 of the *Charter*

S. 8 of the *Charter* guarantees that "[e]veryone has the right to be secure against unreasonable search or seizure."[24] In *Hunter v Southam Inc*, the Supreme Court unanimously agreed that the purpose of s. 8 is to prevent unjustified searches from occurring which can only be accomplished "by a system of prior authorization, not one of subsequent validation."[25] In most

---

ent-doesnt-matter/> [perma.cc/XK8Q-UJC2]; Lee Ann Conrod, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information" (2019) 24 Appeal 115 at 125.

19 *R v Wong*, [1990] 3 SCR 36, 120 NR 34 [*Wong*].

20 *R v Duarte*, [1990] 1 SCR 30, 65 DLR (4th) 240 [*Duarte*].

21 *Mills*, *supra* note 8 at 110.

22 Steven Penney, "*R v Mills*: Sacrificing Communications Privacy to Catch a Predator?" (2019) 54 Crim Reports 1 at 7–8 [Penney, "*R v Mills*"].

23 *Ibid* at 2.

24 *Charter*, *supra* note 1.

25 *Hunter v Southam Inc*, *supra* note 2 at 160.

circumstances, judicial authorization must be obtained for searches and seizures.

Evaluating s. 8 claims is a two-step analysis; the first part of the analysis asks whether there was a search or seizure.[26] A court will determine that the state has conducted a search when it invades an area in which one has a reasonable expectation of privacy. In the context of informational privacy, a search occurs where the state obtains "personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[27] If there was a search, then the second portion of the test evaluates whether the search or seizure was reasonable. In order to be considered reasonable the search must be authorized by law, the law itself must be reasonable, and the manner in which the search is conducted must be reasonable.[28] Warrantless searches are considered *prima facie* unreasonable and the state must rebut this presumption by proving on a balance of probabilities that the search was authorized by law and was conducted in a reasonable manner.[29]

The onus is on the claimant to "establish a reasonable expectation of privacy in the subject matter of the search."[30] This means that the person subjectively expected that the subject matter would be private and that this expectation was objectively reasonable.[31] Courts may infer that unless there is evidence to the contrary, information on a person's cell phone attracts a subjective expectation of privacy.[32] On the other hand, objective reasonability tends to be the point of contention in many s. 8 analyses.[33] Whether the claimant's expectation of privacy was objectively reasonable is assessed using the non-exhaustive list of factors outlined by the Supreme

---

26 *R v Tessling*, 2004 SCC 67 at para 18; *R v Evans*, [1996] 1 SCR 8 at para 11, 131 DLR (4th) 654.

27 Chan, "Text Message Privacy", *supra* note 4 at 70.

28 *R v Collins*, [1987] 1 SCR 265 at 278, 38 DLR (4th) 508.

29 Chan, "Text Message Privacy", *supra* note 4 at 70.

30 *Canfield*, *supra* note 5 at para 59.

31 *Marakah*, *supra* note 11 at para 10; *Southam Inc*, *supra* note 2 at 159–60.

32 *Canfield*, *supra* note 5 at para 62; *R v Fearon*, 2014 SCC 77 at para 51 [*Fearon*].

33 Chan, "Text Message Privacy", *supra* note 4 at 76; Gerald Chan, "Search and Seizure of Private Communications" in Nader Hasan, ed, *Digital Privacy in Canada* (Toronto: LexisNexis Canada Inc, 2018) at 119 [Chan, "Search and Seizure"]; Leonid Sirota, "What was Equilibrium Like?" (31 May 2019), online: *Double Aspect* <doubleaspect.blog/2019/05/31/> [perma.cc/SXS8-EY43] [Sirota, "Equilibrium"].

Court in *R v Edwards*.[34] These factors include possession or control over the property searched, the private nature of the subject matter searched, and the place where the search occurred.[35] In the context of electronic communications, the "place" is not a physical location, but rather the sphere of the electronic conversation.[36] Where an individual's right to privacy has been infringed upon by the state, they may seek a remedy of exclusion under s. 24(2) of the *Charter*.[37]

The proceeding sections will review s. 8 jurisprudence leading up to the decision in *R v Mills*.

B. Early Informational Privacy Cases

The Supreme Court first addressed informational privacy in *R v Plant*.[38] The appellant was accused of having a marijuana-grow-operation. Police obtained his electricity records from his service provider, which he sought to have excluded. The majority found that electricity patterns did not "reveal intimate details of the appellant's life" and therefore were not sufficiently "personal and confidential" to attract protection under s. 8.[39] Justice Sopinka[40] (as he then was) discusses the values underlying s. 8 protection:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include

---

34 Nader Hasan, "Searching the Digital Device" in Gerald Chan & Nader Hasan, eds, *Digital Privacy - Criminal, Civil and Regulatory Litigation* (Toronto: LexisNexis Canada Inc, 2018) at 5; *R v Edwards*, [1996] 1 SCR 128 at para 45, 132 DLR (4th) 31.

35 *Canfield*, *supra* note 5 at para 62; *Marakah*, *supra* note 11 at para 24; *R v Edwards*, *supra* note 34 at para 45.

36 *Marakah*, *supra* note 11 at para 27; Chan, "Text Message Privacy", *supra* note 4 at 72.

37 Chan, "Text Message Privacy", *supra* note 4 at 70.

38 *R v Plant*, [1993] 3 SCR 281, 12 Alta LR (3d) 305 [*Plant*].

39 *Ibid* at 293–94. Justice McLachlin strongly dissented, expressing that the information was not public, the police obtained it through a "special arrangement" and therefore should have been required to obtain a warrant. She disagreed as to the "sufficiently personal" threshold, as the records gave information as to what was happening inside a private dwelling, "the most private of places". She asserts that a reasonable person would conclude that such records should only be used for the purpose for which they were made, not divulged to strangers without legal authorization.

40 With former Chief Justice Lamer and Justices La Forest, Gonthier, Cory, and Iacobucci concurring.

> information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[41]

The idea of a "biographical core" places one's expectation of privacy on a spectrum. Information such as sexual orientation would be considered extremely personal and worthy of protection, whereas preference in hockey team is likely less so.[42]

The subsequent 5-4 split in *R v Gomboc*[43] on the significance of the biographical core creates a patchwork of reasons, resulting in confusion for law enforcement and lower courts alike.[44] Law enforcement requested that the electricity provider install a device which would record power consumption in order to determine whether it was consistent with a grow-operation. This information was used in order to obtain a search warrant for Mr. Gomboc's residence. Justice Deschamp[45] relied on the biographical core principle to determine whether there was a reasonable expectation of privacy. The concurring decisions of Justice Abella[46] and dissenting decision of Chief Justice McLachlin (as she then was)[47] representing five members of the court did not employ the biographical core principle to assert s. 8 protection. This indicates its use is limited in the context of informational privacy.[48] This divergence in reasons creates confusion:

> It is a challenge to prevent a breach when one cannot foresee how a judgment will split and where the majority will fall. When police are left with lengthy split judgments, it is difficult to understand the law. How is the Court going to handle new technology coming when they cannot even agree how to treat utility records?[49]

Similarly, the divergent reasons in *Mills* are also apt to create confusion for lower courts and law enforcement.

---

41 *Plant*, *supra* note 38 at 293–94.
42 Penney, "Digitalization of Section 8", *supra* note 6 at 520.
43 *R v Gomboc*, 2010 SCC 55 [*Gomboc*].
44 Conrod, *supra* note 18 at 125.
45 Justices Charron, Rothstein, and Cromwell concurring.
46 Justices Binnie and LeBel concurring.
47 Also on behalf of Justice Fish.
48 Conrod, *supra* note 18 at 125.
49 *Ibid.*

C. Surveillance and Neutrality

1. Third-Party Surveillance

There are two types of surveillance: third-party and participant. Third-party surveillance is the "capture of communications between two or more parties, none of whom were aware of the capture at the time it occurred", for example, wiretapping.[50] S. 184(1) of the *Criminal Code* makes it an indictable criminal offence to wilfully intercept private communications.[51] The requirements for law enforcement to engage in wiretap operations are stringent. They must establish that there is probable cause to believe that a specified crime has been or will be committed and that the interception will afford evidence of the specified crime.[52] They must also establish investigative necessity.[53] The authorization must be signed by a provincial or federal Attorney General, the Minister of Public Safety, or their respective deputies.[54] In contrast, general warrants only require that the applicant establish reasonable grounds to believe an offence has been or will be committed.[55]

2. Consent Surveillance and the Duarte Principle

The second type of surveillance is participant, or "first party," surveillance wherein one party (such as an undercover officer or informant) is aware that the conversation is being recorded by the state and the other party is not.[56] Participant surveillance was at issue in *R v Duarte*. Police equipped an apartment with audio-equipment that recorded an informant and undercover officer discussing a cocaine transaction with the appellant.[57] The Supreme Court framed the issue as:

> [W]hether our constitutional right to be secure against unreasonable search and seizure should be seen as imposing on the police the obligation to seek prior judicial authorization before engaging in participant surveillance, or whether the police should be entirely free to determine whether circumstances justify recourse

---

50 Penney, "*R v Mills*" *supra* note 22 at 3.

51 *Criminal Code*, RSC 1985, c C-46, s 184(1).

52 *Ibid*, s 186(1)(a) [emphasis added].

53 *Ibid*, s 185(1)(h). In practice, this means disclosing whether other investigative procedures have been tried and failed, or why they are unlikely to succeed, or that urgency renders other investigative techniques impractical.

54 *Ibid*, s 185(1).

55 *Ibid*, s 487.01(a) [emphasis added].

56 Penney, "*R v Mills*", *supra* note 22 at 4.

57 *Duarte*, *supra* note 20.

> to participant surveillance and, having so determined, be allowed an unlimited discretion in defining the scope and duration of participant surveillance.[58]

Prior to the Supreme Court's decision in *Duarte*, participant surveillance operations were exempt from the requirement for judicial authorization.[59] The Court emphasized that the regulation of electronic surveillance prevents not only the risk that our words will be repeated, but protects us against "the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words."[60] The Court found "no logical distinction" between third-party and participant surveillance.[61] The *Duarte* principle dictates that one party consenting to state interception of private communications does not waive the other parties' privacy interest.[62] The effect of the *Duarte* principle is that state must meet the wiretap threshold when obtaining a warrant for participant surveillance.

Similarly, in *R v TELUS Communications Co* (*TELUS*), the Supreme Court found that a general warrant was insufficient for law enforcement to prospectively obtain copies of customers' text message communications. Justice Abella writes: "The only practical difference between text messaging and the traditional voice communications is the transmission process. This distinction should not take text messages outside the protection of private communications to which they are entitled in Part VI."[63] This means that Canadians should be able to maintain the same expectation of privacy in text messages as in telephone calls, which require a wiretap warrant to intercept.

3. The Role of Probable Cause

As the above cases illustrate, the Court has regularly stressed the value of private communications. The *Duarte* principle dictates that participant and third-party surveillance are virtually indistinguishable.[64] Participant surveillance operations require law enforcement to establish probable cause to believe that a specified crime has been or will be committed and that the interception will afford evidence of the crime.[65] The purpose of this high

---

58 *Ibid* at 42.
59 Penney, "*R v Mills*", *supra* note 22 at 4.
60 *Duarte*, *supra* note 20 at 32.
61 *Ibid* at 33.
62 Penney, "*R v Mills*", *supra* note 22 at 5.
63 *R v TELUS Communications Co*, 2013 SCC 16 at para 5 [*TELUS*].
64 *Duarte*, *supra* note 20 at 33.
65 *Criminal Code*, *supra* note 51, s 186(1)(a).

threshold is to prevent the possibility that law enforcement will view recourse to electronic surveillance as a "routine administrative matter."[66] In *Duarte*, the Court held that the requirement for judicial authorization would not hamper police's ability to combat crime, but rather, would ensure that police restrict participant monitoring to cases where they can demonstrate probable cause.[67] In *Mills*, the police engaged in highly personal conversations with Mr. Mills which resulted in the creation of an electronic record. Based on the aforementioned jurisprudence, this should have been classified as participant surveillance.

4. Neutrality

In *R v Wong*[68], the Supreme Court of Canada once again took a firm stance against police surveillance. Mr. Wong was accused of operating a "floating gaming house" from hotel rooms. Police installed a video camera in a room registered to Mr. Wong without prior judicial authorization. The Court frames the issue:

> Accordingly, it follows logically from what was held in *R. v. Duarte* that it would be an error to suppose that the question that must be asked in these circumstances is whether persons who engage in illegal activity behind the locked door of a hotel room have a reasonable expectation of privacy. Rather, the question must be framed in broad and neutral terms so as to become whether in a society such as ours persons who retire to a hotel room and close the door behind them have a reasonable expectation of privacy.[69]

The Court further emphasizes that the *Duarte* principle is not limited to audio equipment but spans to all current and future means the state can use to electronically intrude on individual privacy.[70] Justice LaForest, writing for the majority[71] draws parallels to Orwellian dystopias, warning:

> While there are societies in which persons have learned, to their cost, to expect that a microphone may be hidden in every wall, it is the hallmark of a society such as ours that its members hold to the belief that they are free to go about their daily business without running the risk that their words will be recorded at the sole discretion of agents of the state.[72]

---

66 *Duarte*, *supra* note 20 at 34.
67 *Ibid* at 33–34.
68 *Wong*, *supra* note 19.
69 *Ibid* at 49–50.
70 *Ibid* at 43–44.
71 Of former Chief Justice Dickson and Justices La Forest, L'Heureux-Dubé, and Sopinka.
72 *Wong*, *supra* note 19 at 46.

In *Gomboc*, the Court stressed that the focus of a s. 8 inquiry is not the "nature or identity of concealed items" but rather the "potential impact of the search on the person [or thing] being searched."[73] The decisions in *Duarte, Wong,* and *Gomboc* indicate that engaging in illegal activity does not preclude one's reasonable expectation of privacy under s. 8 of the *Charter*. Later, in *Marakah*, the Supreme Court confirmed once again that s. 8 is to be interpreted in a content-neutral manner.[74]

D. Expectation of Privacy in Digital Devices and Communications

Courts may infer that unless evidence suggests the contrary, information on a person's cell phone attracts a subjective expectation of privacy.[75] In *R v Vu*, the Supreme Court held that a general warrant was insufficient justification for searching a persons' phone.[76] Similarly, in *R v Morelli,* Justice Fish (as he then was) asserts that it would be "difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer."[77] In *R v Cole*, the Supreme Court determined that a reasonable expectation of privacy exists even where there is not complete control over the subject-matter. A tech observed nude photos of a student on Mr. Cole's computer which were subsequently reported to law-enforcement. The Court determined that schools could search staff computers for the purposes of student safety, but law enforcement must still obtain a warrant for the search.[78]

Parallels can be drawn between s. 8 of the *Charter* and the American Fourth Amendment which protects people, their homes, and property against unlawful government search and seizure.[79] The Fourth Amendment

---

73 *Gomboc*, *supra* note 43 at para 39; Penney, "Digitalization of Section 8", *supra* note 6 at 511–12.

74 *Marakah*, *supra* note 11 at para 11.

75 *Canfield*, *supra* note 5 at para 62; *Fearon*, *supra* note 32 at para 51.

76 *R v Vu*, 2013 SCC 60 [*Vu*]; Penney, "Digitalization of Section 8", *supra* note 6 at 515.

77 *R v Morelli*, 2010 SCC 8 at paras 2–3. In that case, a computer technician arrived unannounced at the Appellant's home to perform computer maintenance. The appellant was at home alone with his young daughter. The technician observed child pornography on the computer and immediately left. When he returned the next day, the computer had been "cleaned up". Nevertheless, he reported the issue to law enforcement who took away Mr. Morelli's computers for forensic examination.

78 *R v Cole*, 2012 SCC 53; Penney, "Digitalization of Section 8", *supra* note 6 at 515.

79 In cases such as *Wong* and *Duarte*, the Supreme Court draw parallels to Fourth Amendment Jurisprudence.

is partially prefaced on the idea that "a man's home is his castle."[80] The home is viewed as a zone "beyond the reach of the modern regulatory state."[81] Today, mobile devices are likely to contain even more private information than the home. Electronic conversations can paint a picture of one's financial situation, dating life, deepest thoughts, and insecurities. As Gerald Chan[82] points out, when we sit in the corner of a crowded room tapping away at our phones, "no one has any idea who we are communicating with (or if we are communicating at all)."[83] A similar analysis is put forth by Chief Justice McLachlin (as she then was) in *Marakah*:

> One can even text privately in plain sight. A wife has no way of knowing that, when her husband appears to be catching up on emails, he is in fact conversing by text message with a paramour. A father does not know whom or what his daughter is texting at the dinner table. Electronic conversations can allow people to communicate details about their activities, their relationships, and even their identities that they would never reveal to the world at large, and to enjoy portable privacy in doing so.[84]

Leonid Sirota[85] suggests that the blurring of lines between the spoken and written word leads to dispute over the level of privacy protection that ought to be granted.[86] For example, in *Marakah*, the issue was whether individuals could retain a reasonable expectation of privacy in their text messages once they are sent to and received on another person's device.[87] The Court

---

80 Jonathan L Hafetz, "'A Man's Home is His Castle?': Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries" (2002) 8:2 William & Mary J Race, Gender & Soc Justice 175 at 175.

81 *Ibid* at 176.

82 Gerald Chan is a partner at Stockwoods LLP where he practices criminal, constitutional, and regulatory litigation. He argued the cases of *Fearon*, *Marakah*, *Jones*, and *Mills* before the Supreme Court of Canada.

83 Chan, "Text Message Privacy", *supra* note 4 at 69.

84 *Marakah*, *supra* note 11 at para 36.

85 Leonid Sirota is a constitutional law scholar and the founder of the Double Aspect Blog. He teaches public law and legal philosophy at the Auckland University of Technology where he also directs the LLM program. He has a B.C.L /LL.B from McGill University, as well as an LL.M and J.S.D from the NYU School of Law.

86 Leonid Sirota, "Ceci est-il une conversation?" (13 December 2017), online: *Double Aspect* <doubleaspect.blog/2017/12/13/ceci-est-il-une-conversation/> [perma.cc/66G3-2J4Y].

87 Chan, "Text Message Privacy", *supra* note 4 at 72.

answered the question in the affirmative, in particular as it relates to the state.[88]

In their submissions, the Crown attempted to draw parallels between text messages and letters as only the recipient of a letter has standing to challenge its search and seizure.[89] This argument was rejected by the Court, Chief Justice McLachlin reiterated that per *Wong*, s. 8 is meant to keep pace with technological development.[90] Instead, text messages were characterized as a "digital conversation", given the quantity of information they contain and the speed at which messages are transmitted.[91] The "place of the search" is the private electronic space created between the two parties to the conversation, and "control" is to be understood as the individual freedom to determine how, when, and to whom the sender discloses their information.[92]

Recall that the parties were corresponding about the sale of illegal firearms. Despite this fact the Supreme Court did not place a value-judgement on "Marakah's bad choice of friends or even worse, his bad judgment to deal drugs."[93] The fact that the parties were communicating about illegal activity was irrelevant to the s. 8 analysis.[94] This evaluation is consistent with *Duarte* and *Wong*.

The majority in *Marakah* held that parties obtain a reasonable expectation of privacy in their electronic communications, regardless of whether the police search the sender or recipient's device.[95] In its companion case *Jones*, the Court expanded upon their decision in *TELUS*. They clarified that police require a production order to obtain copies of historical text messages from service providers but must meet the requirements for a wiretap authorization when obtaining messages prospectively.[96] The differentiation was justified by the fact that allowing

---

88 *Ibid*.

89 *Ibid* at 73; *Marakah*, *supra* note 11 at paras 86–87.

90 *Marakah*, *supra* note 11 at para 86; *Wong*, *supra* note 19 at 44.

91 *Marakah*, *supra* note 11 at para 87.

92 Chan, "Text Message Privacy", *supra* note 4 at 72–73.

93 Lisa Silver, "A Look Down the Road Taken by the Supreme Court of Canada in R v Mills" (5 May 2019), online: *CanLii Connects* <canliiconnects.org/en/commentaries/66706> [perma.cc/V4U8-YQ34].

94 *Marakah*, *supra* note 11 at paras 11, 54.

95 Chan, "Text Message Privacy", *supra* note 4 at 70.

96 *Ibid*. See also *Jones*, *supra* note 12; *TELUS*, *supra* note 63.

police surveillance of future messages under a general warrant alone could tempt the state into engaging in fishing expeditions.[97]

In *Marakah*, Chief Justice McLachlin indicates that s. 8 protections are not only applicable to text messages but extend to "technologically distinct" but "functionally equivalent" means of messaging such as iMessage and Blackberry Messenger.[98] On the other hand, communications shared to the digital "public square" such as social media posts and chatrooms are unlikely to fall under the umbrella of s. 8 protection.[99]

E. *R v Mills*

1. Background

In 2012, two separate officers of Royal Newfoundland Constabulary (RNC) created Hotmail and Facebook accounts posing as 14-year-old girls. Mr. Mills initiated contact with "Leann" (the first fake account) through Facebook. The RNC took screenshots of the conversations. The officers created a second account "Julie" who then initiated contact with Mr. Mills.[100] In order to make the profile appear more legitimate, the officers also communicated with minors who interacted with LeAnn's profile and provided their personal information to the officers.[101] Eventually Mr. Mills and "Leann" agreed to meet in a park, where Mr. Mills was arrested and charged with child-luring. At issue was whether this investigative technique amounted to a search or seizure under s. 8 of the *Charter*, and whether the police had intercepted a private communication without prior judicial authorization.[102]

While this decision is technically "unanimous", it is anything but. All justices reached the conclusion that the messages should be admitted, but for wholly different reasons. As Peter McCormick writes: "Putting the point as starkly as possible: the outcome really matters only to the immediate parties, but the reasons matter to everybody. This is because it is the reasons, not the outcome, that constitute the precedent that constrains the

---

97 Chan, "Text Message Privacy", *supra* note 4 at 80–81.

98 *Marakah*, *supra* note 11 at para 18.

99 Penney, "*R v Mills*", *supra* note 22 at 5.

100 *R v Mills*, [2014] NJ No 392 at paras 3–12, 2014 CarswellNfld 392; *Mills*, *supra* note 8 at paras 5–7.

101 Samuelson-Glushko, *supra* note 9 at 11.

102 *Mills*, *supra* note 8 at para 1.

immediate court and instructs the lower courts."[103] The reasons in *Mills* are highly divergent and apt to cause confusion for lower courts.

2. Reasoning

Justice Brown writes for himself, Justices Abella and Gascon forming a "majority". They found that Mr. Mills could not claim an objectively reasonable expectation of privacy when "communicating with someone he believed to be a child, who was a stranger to him."[104] Justice Brown characterizes objective reasonableness as a "normative question about when Canadians ought to expect privacy given the applicable considerations. On a normative standard, adults cannot reasonably expect privacy online with children they do not know."[105] Justice Brown justifies departing from the standard of content neutrality based on the fact that the police knew that the relationship was fictitious and therefore LeAnn was a "stranger" to Mr. Mills.[106]

Justice Karakatsanis, writing for herself and Chief Justice Wagner found that there was no search or seizure, and thus no need to undertake a s. 8 analysis. She writes "because it is not reasonable to expect that your messages will be kept private from the intended recipient (even if the intended recipient is an undercover officer)."[107] The conversation "necessarily took place in a written form", therefore the screen captures were a mere copy of a written record, not a separate and surreptitious permanent record created by the state.[108] She attempts to distinguish the case from *Duarte* by suggesting that participants in electronic conversations know that the record will be created and create it themselves as opposed to the state doing so.[109]

Justice Moldaver found the reasons of both Justice Brown and Justice Karakatsanis "sound in law" forming a proper basis for dismissing Mr. Mills' appeal.[110]

Justice Martin frames the issue as whether it would be reasonable for those in a free and democratic society to expect that the state will only access

---

103 McCormick, *supra* note 18.
104 *Mills*, *supra* note 8 at para 22.
105 *Ibid*.
106 *Ibid* at paras 20, 22, 27.
107 *Ibid* at paras 36–37.
108 *Ibid* at paras 36–37, 45.
109 *Ibid* at para 47.
110 *Ibid* at paras 66–67.

electronic recordings of private communications where they have sought the authorization to do so.[111] Justice Martin departs from her colleagues in determining that a search occurred, and that because that search occurred without a warrant, it was unreasonable.[112] Individuals have a reasonable expectation that surreptitious electronic recordings of their communications cannot be acquired by the state at its sole discretion.[113]

Justice Martin recognizes that means of communication have shifted from oral to text-based conversations. In fact, written electronic communications are a "virtual prerequisite" for participation in modern society.[114] This shift should not waive the state's duty to obtain prior judicial authorization in order to access electronic recordings of private communications. She asserts that this duality should "support, not undermine the protection of privacy rights, because a recording exists and the state has unrestricted and unregulated access to it."[115] Given that electronic conversations have "characteristics of permanence, evidentiary reliability, and transmissibility", she characterizes them as analogous to surreptitious electronic recordings.[116]

Although Justice Martin found that Mr. Mills' s. 8 rights were infringed, she would have allowed the evidence under s. 24(2) given that the seriousness of the breach was minimal and excluding the evidence would bring the administration of justice into disrepute.[117]

III. Implications of the *Mills* Decision

A. Overturning or Equilibrium?

In *Marakah*, Chief Justice McLachlin (as she then was) asserts that "the fruits of a search cannot be used to justify an unreasonable privacy violation."[118] Similarly, the nature of the crime in *Mills*, though abhorrent, cannot be used to justify the Supreme Court's departure from decades of precedent. In the limited literature regarding *R v Mills*, two distinct schools

---

111 *Ibid* at para 133.
112 *Ibid* at para 76.
113 *Ibid* at para 72.
114 *Ibid* at para 96.
115 *Ibid* at para 93.
116 *Ibid* at para 91.
117 *Ibid* at para 149.
118 *Marakah*, *supra* note 11 at para 48.

of thought have emerged. Professor Steven Penney[119] argues that the reasons of Justices Brown and Karakatsanis effectively overturn the principles established in *Duarte* and *Marakah*.[120] Sirota disagrees with this analysis and characterizes the *Mills* decision as an attempt at equilibrium adjustment.[121]

Equilibrium adjustment theory suggests that states will calls on courts to restore the technological status quo.[122] As Kerr writes:

> Equilibrium-adjustment acts as a correction mechanism. When judges perceive that changing technology or social practice significantly weakens police power to enforce the law, courts adopt lower Fourth Amendment protections for these new circumstances to help restore the status quo ante. On the other hand, when judges perceive that changing technology or social practice significantly enhances government power, courts embrace higher protections to counter the expansion of government power. The resulting judicial decisions resemble the work of drivers trying to maintain constant speed over mountainous terrain. In an effort to maintain the preexisting equilibrium, they add extra gas when facing an uphill climb and ease off the pedal on the downslopes. [123]

In *Duarte*, Chief Justice Dickson (as he then was) writes: "A reasonable balance must therefore be struck between the right of individuals to be left alone and the right of the state to intrude on privacy in furtherance of its responsibilities for law enforcement."[124] This concept of balance is oft repeated in s. 8 jurisprudence.

Both the *Marakah* and *Mills* decisions are attempts at equilibrium adjustment. In *Marakah*, the Court "intended to preserve the previously undoubted privacy of the exact content of personal conversations" whereas in *Mills* the Court sought to retain some distinction between oral and electronic communications.[125] Sirota suggests that all justices in the *Mills* decision frame their reasons as a means to "preserve or restore a balance of privacy that these developments threaten to disrupt."[126] He points to Justice

---

119 Steven Penney obtained an LL.M. from Harvard Law and is a professor of various criminal law topics at University of Alberta. He researches, teaches, and consults in the areas of criminal procedure, evidence, substantive criminal law, privacy, technology.

120 Steven Penney, "'To Catch a Predator' Reasonable Expectations of Privacy in R v Mills" (23 April 2019), online: *University of Alberta, Faculty of Law Blog* <ualbertalaw.typepad.com/faculty/2019/04/to-catch-a-predator-reasonable-expectations-of-privacy-in-r-v-mills.html> [perma.cc/55W3-YQEJ] [Penney, "Reasonable Expectations"].

121 Sirota, "Equilibrium", *supra* note 33.

122 Kerr, *supra* note 7.

123 *Ibid* at 487–88.

124 *Duarte*, *supra* note 20 at 41–42.

125 Sirota, "Equilibrium", *supra* note 33.

126 *Ibid*.

Brown's contention that the means used in *Mills* "would not significantly reduce the sphere of privacy enjoyed by Canadians."[127] He describes Justice Karakatsanis' reasons as "less explicit" in her effort at adjustment. She insisted that written communications should not be treated as akin to oral communications and that any alternative conclusion would "significantly and negatively impact police undercover operations, including those conducted electronically."[128] Sirota interprets Justice Martin's decision as suggesting that "regardless of the parties' status, and all conversations, regardless of the means used to carry them out, were entitled to privacy protections."[129] Sirota agrees with Justice Karakatsanis that an electronic conversation between a suspect and undercover officer is not a meaningfully greater intrusion on privacy than if it were to occur in person.[130]

In prior s. 8 cases, the Crown has called on the Court to restore the status quo through the use of backward-looking analogies. In *Duarte*, the Crown suggested that the use of recording-equipment was merely an expansion on the memory capacity of police.[131] In *Vu*, the Crown compares information stored on phones to that stored in filing cabinets or cupboards.[132] In *Marakah*, the Crown compared text messages to sending letters.[133] All of these arguments were summarily rejected by the Court. Despite this fact, in the *Mills* decision Justice Karakatsanis still compares electronic conversations to letters writing "if Mills had sent a letter or passed a note to an undercover officer, s. 8 would not require the officer to get a warrant prior to reading it."[134] This is far from the only conflict between the *Mills* decision and prior s. 8 jurisprudence.

Professor Penney argues that the *Mills* decision has effectively overturned *Duarte* and *Marakah*.[135] The *Duarte* principle has held steady for over three decades, covering both telephone and in-person conversations, even where one party consents to the recording.[136] Penney argues that the investigative technique used in *Mills* differs from *Duarte* only insofar that

---

127 *Ibid*. See also *Mills*, *supra* note 8 at para 20.

128 *Mills*, *supra* note 8 at para 52; Sirota, "Equilibrium", *supra* note 34.

129 Sirota, "Equilibrium", *supra* note 34.

130 *Ibid*.

131 *Duarte*, *supra* note 20 at 41–42.

132 *Vu*, *supra* note 76 at paras 1, 24.

133 *Marakah*, *supra* note 11 at paras 86–87.

134 *Mills*, *supra* note 8 at para 45.

135 Chan, "Search and Seizure", *supra* note 33 at 120.

136 Penney, "*R v Mills*", *supra* note 22 at 5.

the communications were electronic text as opposed to oral statements.[137] If the undercover officer were communicating with Mr. Mills by phone, they would have been required to obtain prior judicial authorization to record the call.[138] The only factor distinguishing *Mills* from *TELUS* is that law enforcement effectively cut out the middleman by engaging in the conversation.[139] The police were thus engaging in participant surveillance, which per *Duarte*, is not legally distinct from third-party surveillance.

Penney disputes Justice Karakatsanis' contention that because messages are automatically recorded, the expectation of privacy within them is lower.[140] In fact, such an argument was already rejected by the Supreme Court in *Marakah* in recognizing the inherently private nature of text messages.[141] Justice Martin is also skeptical of this argument, asserting that the electronic recording of personal communications should support rather than undermine the protection of privacy rights.[142] She argues that "A general proposition that it is not reasonable for individuals to expect that their messages will be kept private from the intended recipient cannot apply when the state has secretly set itself up as the intended recipient."[143] This contention is highly reasonable. Mills' conduct and expectation of privacy would be based on his assumption that he was interacting with another private individual.[144] Justice Martin characterizes Justice Karakatsanis' finding that s. 8 was not engaged because of state participation as undermining the purpose of privacy rights.[145]

B. The Stranger Exception and Content Neutrality

A person is able to operate an illegal gambling ring behind a closed hotel door, yet still maintain an expectation of privacy under s. 8 of the *Charter*.[146] A person can converse (either in person or through text) about trafficking without fear of their words being recorded at the sole discretion

---

137 *Ibid*.
138 Chan, "Text Message Privacy", *supra* note 4 at 81.
139 *Ibid* at 82.
140 Penney, "*R v Mills*", *supra* note 22 at 5.
141 Penney, "Reasonable Expectations", *supra* note 120 at 5–6.
142 *Mills*, *supra* note 8 at para 93.
143 *Ibid* at para 101.
144 Samuelson-Glushko, *supra* note 9 at 10.
145 *Mills*, *supra* note 8 at para 107.
146 *Wong*, *supra* note 19.

of police.[147] Yet, an adult conversing with youth online could be opening themselves up to a judicial analysis as to the social value of their relationship.

Both Penney and Sirota agree that Justice Brown's decision is narrower in scope. S. 8 protection does not apply to text communications with strangers believed to be children.[148] However, the term "stranger" is ambiguous.[149] When does an online persona transition from being a stranger to being familiar? Is an offline-world meeting required or are prior oral conversations (with or without video) sufficient? What level of identity verification is required?[150]

Mills' not having met the undercover officer in person is the only distinguishing factor between *Mills* and *Marakah*. Chan argues that not having met someone in person should not negate a reasonable expectation of privacy. He points to online dating, seeking medical advice from online doctors, and prospective e-mails between clients and lawyers as intensely private online conversations.[151] Not protecting these communications because the participants had never met in person would result in a bizarre outcome.[152] Today, communications cannot be "neatly separated into 'offline' and 'online' boxes." To treat text conversations between strangers differently would be "anachronistic" in an age of increasing levels of online communication between people who have never met.[153]

Justice Martin is also unimpressed with Justice Brown's stranger exception. She explains that the value of a personal relationship is not an appropriate object of a s. 8 inquiry.[154] A reading of s. 8 indicates that the right is guaranteed to <u>everyone</u> and it is not the court's role to analyze those relationships with a view of denying protection to certain classes of people.[155] To find otherwise would be to put "courts in the business of evaluating personal relationships" and entirely disregards content neutrality.[156] Justice Martin writes:

---

147 *Marakah*, *supra* note 11; *Duarte*, *supra* note 20.

148 Penney, "*R v Mills*", *supra* note 22 at 6; Sirota, "Equilibrium", *supra* note 33.

149 Penney, "*R v Mills*", *supra* note 22 at 5.

150 *Ibid* at 6.

151 Chan, "Text Message Privacy", *supra* note 4 at 81.

152 *Ibid*.

153 Chan, "Search and Seizure", *supra* note 33 at 120.

154 *Mills*, *supra* note 8 at para 129.

155 *Ibid*.

156 *Ibid* at para 110.

> Indeed, this concept of "relationship" is built upon two ideas that have already been rejected by this Court. First, the concept of "relationship" is really a proxy for "control" and is based in risk analysis reasoning that this Court has rejected. Second, "relationship" is also used to target illegal activity, and is not therefore content neutral.[157]

She concludes that it is inappropriate to insert judicial (dis)approbation of an accused's lifestyle into the s. 8 analysis. Courts should not create "*Charter*-free zones" in certain people's communications on the basis that they may be criminals whose relationships are not socially valuable.[158] Chan suggests the issue should be framed as whether Canadians have an expectation of privacy in their electronic messages, not whether there is an expectation of privacy in the message's illegal content.[159] This proposition is consistent with prior Supreme Court jurisprudence such as *Marakah* which roots privacy expectations in the private electronic conversation, as opposed to conversations between criminals or about crime.[160]

The crime of "child luring" is quite rare with only 122 cases occurring in Canada between 2011 and 2019.[161] Despite being rare, the crime of child luring creates a serious risk of harm for victims. In her judgement, Justice Martin turns her mind to this fact:

> The sexual exploitation of a minor is an abhorrent act that Canadian society, including this Court, strongly denounces. In an online context, adults who prey on children and youth for a sexual purpose can gain the trust of these young people through anonymous or falsified identities, and can reach into their homes more easily than ever before, from anywhere in the world. Children and youth are therefore particularly vulnerable on the internet and require protection.[162]

There is no doubt that society has an interest in protecting children from sexual predation. Yet, there is little evidence to suggest that accused captured by these stings would have perpetuated child luring offences on real victims without police intervention. In contrast, "the evidence demonstrates that police contact likely induced the offence."[163] Further, proactive investigations allow officers to co-create the evidence they need to

---

157 *Ibid*.

158 *Ibid* at paras 110–11.

159 Chan, "Search and Seizure", *supra* note 33 at 121.

160 Samuelson-Glushko, *supra* note 9 at 9.

161 Lauren Menzies & Taryn Hepburn, "Harm in the Digital Age: Critiquing the Construction of Victims, Harm, and Evidence in Proactive Child Luring Investigations" (2020) 43:3 Man LJ at 398.

162 *Mills*, *supra* note 8 at para 69.

163 Menzies & Hepburn, *supra* note 161 at 28.

secure a conviction.[164] This could have the effect of artificially inflating the perceived risk of child-victimization and unnecessarily increasing public anxiety.[165] By framing s. 8 in terms of societal expectations, the Court put themselves in the position of policing morality. Instead of disregarding content neutrality in s. 8, the Court could have addressed the public's interest under s. 24(2), as Justice Martin did. Justice Martin found that to exclude "relevant and reliable evidence in a child-luring case" would bring the administration of justice into disrepute.[166]

C. The Potential Chilling Effects of *Mills*

The Supreme Court has long recognized the correlation between privacy and freedom of expression. For example, Chief Justice Dickson wrote in *Canada (Human Rights Commission) v Taylor*, "the freedoms of conscience, thought and belief are particularly engaged in a private setting."[167] As Chan eloquently states: "Private communications are where we experiment with embryonic ideas, share our intimate thoughts, and express our rawest emotions."[168] The inherently private nature of online communications was recognized by Chief Justice McLachlin in *Marakah*, providing the example of a wife being unaware her husband was conversing with a paramour.[169] As the Court expressed in *Duarte*, "Countenancing participant surveillance, strikes not only at the expectations of privacy of criminals but also undermines the expectations of privacy of all those who set store on the right to live in reasonable security and freedom from surveillance, be it electronic or otherwise."[170]

The "child stranger" exception put forth in *Mills* could have the effect of chilling legitimate and socially beneficial online conversations:

> If these adults are aware (as they presumably will be after *Mills*) that a minor seeking to communicate with them might actually be a police officer, they will be less likely to enter into such conversations in the first place, reasonably fearing the disclosure of intimate (and potentially stigmatizing) personal information.[171]

---

164 *Ibid* at 29.

165 *Ibid* at 18–19, 28.

166 *Mills*, *supra* note 8 at para 155.

167 Chan, "Text Message Privacy", *supra* note 4 at 71; *Canada (Human Rights Commission) v Taylor*, [1990] 3 SCR 892, 75 DLR (4th) 577.

168 Chan, "Text Message Privacy", *supra* note 4 at 71.

169 *Marakah*, *supra* note 11 at para 36.

170 *Duarte*, *supra* note 20 at 34.

171 Penney, "Reasonable Expectations", *supra* note 120 at 8.

Similarly, Justice Martin found that the exemption would cast "suspicion on an entire category of human relationship" thus exposing meaningful relationships to unregulated electronic surveillance.[172] Justice Martin provides several examples of these beneficial relationships such as adults providing guidance to youth who are struggling with addictions, bullying, or their sexual identity.[173]

One such example of a socially beneficial relationship would be LGBTQ+ youth who receive online support from LGBTQ+ adults. A 2017 study found that LGBTQ youth use Facebook to explore new friendships and relationships, but do not commonly use the platform to meet people. Participants reported feeling more comfortable communicating through social media. The platform provided a safe space for youth to both seek support and explore their gender / sexual identities.[174] Youth may wish to hear others' experiences coming out to their family, and for those with a difficult living situation, whether life improved upon moving out of their childhood home. The adult may be one of the few people that the youth can turn to for support.[175]

Similarly, proactive child-luring investigations can intrude upon legitimate online spaces where adults seek to express their sexuality. Officers may hold a bias against a particular sexual preference (such as BDSM) or sexual orientation leading them to inflate risk of harm. For example, in *R v Gowdy*, officers in a rural area responded to an ad from someone looking for a "young" guy "under 35", such as a "married" or "college guy" who was open to receiving fellatio.[176] Clearly, the terms "married" and "college guy" are inconsistent with seeking a sexual relationship with a minor. Menzies and Hepburn suggest that police were not aiming to protect youth but were instead "responding to Gowdy's sexuality in a small town."[177] Similarly, police have set up operations on kink sites which only allow users over the age of eighteen, as well as adult-only escort sites.[178] The purported aim of these operations is to "protect children", yet, the investigations are

---

172 *Mills*, *supra* note 8 at para 126; Penney, "*R v Mills*", *supra* note 22 at 7.

173 *Mills*, *supra* note 8 at paras 122–26.

174 Leanna Lucero, "Safe Spaces in online places: social media and LGBTQ youth" (2017) 9:2 Multicultural Education Rev 117.

175 Penney, "*R v Mills*", *supra* note 22 at 7.

176 *R v Gowdy*, 2014 ONCJ 592; Menzies & Hepburn, *supra* note 161 at 14.

177 Menzies & Hepburn, *supra* note 161 at 14.

178 *Ibid* at 15, 29.

occurring in spaces where predators are unlikely to be looking for victims.[179] The effect is the policing of legitimate online sexual expression based on what individual officers deem to be moral.[180]

Professor Penney expressed concern that adults may be reluctant to support youth online for worry that they may be speaking with an undercover officer.[181] Conversely, would marginalized youth continue to seek support from adult "strangers" with the knowledge that their conversation could be open to state scrutiny? Would adult members of marginalized sexual communities feel comfortable seeking online communication with other adults, knowing that the person on the other end could be a police officer? What justification is there in a free and democratic society for denying such intimate interactions an expectation of privacy?[182]

IV. ELECTRONIC SURVEILLANCE MUST BE REGULATED

Based on the decisions in *Wong*, *Duarte*, *TELUS*, and *Marakah*, law enforcement's activity in *Mills* should have been characterized as participant surveillance. In order to conduct participant surveillance operations, law enforcement must establish that there is probable cause to believe that a specified crime has been or will be committed and that the interception will afford evidence of the crime.[183] The probable cause threshold recognizes that intrusion into Canadians' private lives should not be considered a routine matter.[184] In *Duarte*, the Court held that requiring a warrant to engage in participant surveillance would not hamper police ability to combat crime. Instead, a warrant would ensure police restrict participant monitoring to cases where they can demonstrate probable cause.[185]

In contrast, allowing the police to undertake such operations in an unregulated manner is bound to have consequences:

> A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our

---

179 *Ibid* at 29.
180 *Ibid* at 4, 6.
181 Penney, "Reasonable Expectations", *supra* note 120 at 8.
182 Samuelson-Glushko, *supra* note 9 at 10.
183 *Criminal Code*, *supra* note 51, s 186(1)(a).
184 *Duarte*, *supra* note 20 at 34.
185 *Ibid* at 33–34.

> mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.[186]

There is a risk that such warrantless investigations could have a chilling effect on legitimate online conversations. Technology allows for easy scalability of these operations. This creates the risk of their being seen as "routine" matters. The effect of *Mills* is to allow police to create as many virtual child profiles as they wish enticing people to unwittingly converse with them, and all without any oversight.[187] Is the breaking point 100, 1000 or 100,000 profiles?[188]

As Justice Martin writes in *Mills* "[t]o be constitutionally compliant, state acquisition in real-time of private electronic communications requires regulation."[189] Such regulation is "necessary to preserve the quantum of communications privacy that Canadians enjoyed in the pre-digital era."[190] Requiring a warrant to undertake participant surveillance in the context of online conversations aligns with s. 8 jurisprudence and would not unduly impact police's ability to combat crime.

To leave these operations unregulated leaves room for abuse. In the case of *Mills*, the officer had no clear policies to guide his investigation. Instead, he "created policy on his own, with undesirable consequences."[191] The officer communicated with minors in order to give the fake profile an air of legitimacy.[192] Such proactive investigations can "cast a wide net of electronic surveillance, resulting in innocent members of the public, many of whom may be youth, unwittingly sharing sensitive personal information with the police."[193] As previously mentioned, this can lead to officers disproportionately targeting marginalized sexual communities such as BDSM enthusiasts. Further, a lack of regulation creates potential for officers to use the guise of anonymity to create trust-based online relationships with vulnerable minors. Even if the conversations are not inappropriate in content, the act of deceiving a minor into communication is reprehensible. If not prohibited, at minimum, this practice should be subject to significant oversight.

---

186 *Ibid* at 44.
187 Penney, "*R v Mills*", *supra* note 22 at 7.
188 *Ibid*.
189 *Mills*, *supra* note 8 at 143.
190 Penney, "*R v Mills*", *supra* note 22 at 3.
191 *Mills*, *supra* note 8 at para 147.
192 Samuelson-Glushko, *supra* note 9 at 11.
193 *Mills*, *supra* note 8 at para 147.

Proactive child luring investigations purportedly aim to protect minors from harm. However, in the context of internet communications, rather than being characterized as "victims", teenage girls are often considered "sexual provocateurs putting men at risk of prosecution."[194] Proactive child-luring investigations allow officers to play into an "ideal victim" stereotype. The typical "victim" is portrayed as being "naive, curious, interested in trying various sexual activities, highly agentic and independent, and, depending on their age, often somewhat experienced."[195] These operations contribute to the characterization of adolescent girls as hypersexualized, willing participants.[196]

In *Mills*, the officer used photos he obtained from the internet of a young girl. The girl did not know about this investigation, nor did she consent to the use of her photo. Thus, she was "unwittingly conscripted into a police investigation."[197] Impersonating a young woman online without her consent could potentially lead to harm in both the cyber, and "real" worlds. Social media profiles create lasting first impressions. Use of an individual's photo in conjunction with sexually explicit messaging could result in reputational damage or barriers to finding future employment.[198] Further, use of the photo could expose its subject to cyber-stalking or harassment. For example, in 2013 a San Diego woman was stalked after a fake account used her photo.[199]

These operations should be governed by existing wiretap regulations. Police claim that requiring a warrant would inhibit their investigations.[200] This is completely false. Recall that in *Marakah*, Chief Justice McLachlin (as she then was) implies that communications occurring in the digital "public square" such as social media posts and chatrooms are unlikely to fall under the umbrella of s. 8 protection.[201] Following this logic, police could begin

---

194 Jane Bailey & Valerie Steeves, "Will the Real Digital Girl Please Stand Up? Examining the Gap Between Policy Dialogue and Girls' Accounts of Their Digital Existence" in Hille Koskela, ed, *New Visualities, New Technologies: The New Ecstasy of Communication* (Taylor & Francis Group, 2013) 41 at 54.

195 Menzies & Hepburn, *supra* note 161 at 12.

196 *Ibid* at 4, 12.

197 *Mills*, *supra* note 8 at para 147.

198 Colleen M Koch, "To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation" (2017) 88:1 U Colo L Rev 233 at 243.

199 *Ibid* at 244.

200 Chan, "Search and Seizure", *supra* note 33 at 129.

201 Penney, "*R v Mills*", *supra* note 22 at 5.

their operations in chatrooms without a need to establish any probable cause, and then retain a warrant once the communication moves to a private medium.[202] In fact, many child luring sting operations already proceed in this manner.[203] Further, law enforcement may avail themselves of other methods to combat child luring, including relying on the complaints of inappropriate contact from parents, teachers and children.[204]

V. CONCLUSION

Prior to the *Mills* decision, the Supreme Court routinely took a firm stance against state surveillance. Further, it was a well-established principle that a privacy interest exists in conversations, regardless of the criminal content therein. The *Mills* decision has the potential to confuse lower courts and law enforcement, not just because the justices diverge in their reasoning, but also because it contradicts prior s. 8 jurisprudence. For example, the *Mills* decision evaluates the s. 8 claim in the context of relationships. This has the effect of removing content neutrality from the decision and puts the Court in the position of determining which relationships are worthy of protection. Justice Brown suggests that the stranger exception will only apply in a narrow set of circumstances. It would be prudent for future researchers to undertake a systematic review of post-*Mills* jurisprudence to determine whether this is in fact the case. Points of inquiry could include how frequently law enforcement rely on these types of operations and whether the *Mills* framework permits these proactive operations in other contexts such as drug-trafficking.

Prior jurisprudence such as *Duarte* and *TELUS* lend support to the theory that these types of operations are participant surveillance and thus should require prior judicial authorization. By determining that s. 8 was not engaged in *Mills*, the Court effectively exempted law enforcement from any meaningful regulation when engaging in these types of stings. The consequence of this decision may be an increase in electronic state surveillance and subsequent chilling of online communications. For example, marginalized youth seeking support online may feel less comfortable engaging with an adult "stranger" knowing that their communication could be open to state scrutiny.

---

202 Chan, "Search and Seizure", *supra* note 33 at 129.
203 Chan, "Text Message Privacy", *supra* note 4 at 83.
204 Penney, "*R v Mills*", *supra* note 22 at 7.

The officers' communication with other minors in *Mills* was exploitative, lending support to the conclusion that such operations must be regulated. Existing wiretap provisions are sufficient to regulate these operations and limit the investigations in time and scope. Further, these provisions would prevent law enforcement from embarking upon fishing expeditions made easier by the scalability of this technique.

While some argue that the *Mills* decision is merely the Court's attempt at restoring equilibrium, such action was unnecessary and disproportionate to the consequences. Child luring cases are rare. There is little evidence to suggest that accused caught in proactive investigations would have committed child luring offences against real victims. Officers have other less intrusive means available to them to pursue these types of investigations. Leaving this practice unregulated renders these investigations open to abuse. In other words, the ends do not justify the means.