SUPREME COURT OF CANADA

CITATION: R. *v.* Mills, 2019 SCC 22

APPEAL HEARD: May 25, 2018
JUDGMENT RENDERED: April 18, 2019
DOCKET: 37518

BETWEEN:

Sean Patrick Mills
Appellant

and

Her Majesty The Queen
Respondent

- and -

Director of Public Prosecutions, Attorney General of Ontario, Director of Criminal and Penal Prosecutions, Attorney General of British Columbia, Attorney General of Alberta, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, Canadian Civil Liberties Association, Criminal Lawyers' Association and Canadian Association of Chiefs of Police
Interveners

CORAM : Wagner C.J. and Abella, Moldaver, Karakatsanis, Gascon, Brown and Martin JJ.

REASONS FOR JUDGMENT: (paras. 1 to 35)	Brown J. (Abella and Gascon JJ. concurring)
CONCURRING REASONS: (paras. 36 to 65)	Karakatsanis J. (Wagner C.J. concurring)
CONCURRING REASONS: (paras. 66 to 67)	Moldaver J.
CONCURRING REASONS: (paras. 68 to 159)	Martin J.

Sean Patrick Mills *Appellant*

v.

Her Majesty The Queen *Respondent*

and

Director of Public Prosecutions,
Attorney General of Ontario,
Director of Criminal and Penal Prosecutions,
Attorney General of British Columbia,
Attorney General of Alberta,
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic,
Canadian Civil Liberties Association,
Criminal Lawyers' Association and
Canadian Association of Chiefs of Police *Interveners*

Indexed as: R. *v.* Mills

2019 SCC 22

File No.: 37518.

2018: May 25; 2019: April 18.

Present: Wagner C.J. and Abella, Moldaver, Karakatsanis, Gascon, Brown and Martin JJ.

ON APPEAL FROM THE COURT OF APPEAL FOR NEWFOUNDLAND AND LABRADOR

Constitutional law — Charter of Rights — Search and seizure — Child luring — Police sting operation — Interception with consent — Accused charged with child luring after communicating online with police officer posing as 14-year-old girl — Police using screen capture software to create record of online communications — Whether investigative technique amounted to search or seizure of accused's online communications — Whether police intercepted private communication without prior judicial authorization — Canadian Charter of Rights and Freedoms, s. 8 — Criminal Code, R.S.C. 1985, c. C-46, s. 184.2.

A police officer posed online as a 14-year-old girl named Leann, with the intent of catching Internet child lurers. Using Facebook and Hotmail, M sent Leann sexually explicit messages and arranged a meeting in a park, where he was arrested and charged with child luring. Without having obtained prior judicial authorization, the officer used screen capture software to create a record of his online communications with M as evidence for trial. M applied for the exclusion of the evidence. The trial judge found that the messages were "private communications" as defined in s. 183 of the *Criminal Code* and that prior judicial authorization to capture the messages under s. 184.2 of the *Criminal Code* was therefore required from the point at which the police had determined that M had a potentially inappropriate interest in a minor. He also held that the use of the screen capture software generated a seizure of the communications, and that M had an expectation of privacy in his communications. He therefore found that the police breached s. 8 of the *Charter*.

However, he found that admitting the evidence would not bring the administration of justice into disrepute and he convicted M. The Court of Appeal held that the trial judge had erred in concluding that authorizations under s. 184.2 were required and found that M's expectation of privacy was not objectively reasonable. It held that M's s. 8 rights were not infringed and therefore upheld the conviction.

Held: The appeal should be dismissed.

Per Abella, Gascon and **Brown** JJ.: Section 8 of the *Charter* was not engaged when the officer captured M's electronic communications. To claim s. 8's protection, an accused must show a subjectively held and objectively reasonable expectation of privacy in the subject matter of the putative search. M could not claim an expectation of privacy that was objectively reasonable because M was communicating with someone he believed to be a child, who was a stranger to him, and the investigatory technique meant that the undercover officer knew this when he created her. On the facts of this case, giving judicial sanction to the particular form of unauthorized surveillance in question would not see the amount of privacy and freedom remaining to citizens diminished to a compass inconsistent with the aims of a free and open society, if expectations of privacy are to express a normative, rather than descriptive, standard. Therefore, the sting did not require prior judicial authorization.

Objective reasonableness is assessed in the totality of the circumstances, along four lines of inquiry. The first three inquiries are an examination of the subject

matter of the alleged search, a determination as to whether the claimant had a direct interest in the subject matter and an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter. These lines of inquiry support M's claim to an expectation of privacy. The subject matter is the electronic communications, and they have no legally significant distinction from text messages. M intended to have a one-on-one online conversation. As a participant and a co-author of the communications, M had a direct interest in the subject matter and he expected the communications to be private.

The fourth inquiry is whether M's subjective expectation of privacy was objectively reasonable having regard to the totality of the circumstances. Determining objective reasonableness is 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. This appeal involves a particular set of circumstances, where the nature of the relationship and the nature of the investigative technique are decisive. Although s. 8 is not traditionally approached from the perspective of the particular relationship because its protection is content-neutral, the police knew the relationship in advance of any potential privacy breach. While society values many adult-child relationships as worthy of s. 8's protection, this relationship is not one of them. With respect to the investigative technique, the police knew from the outset that the relationship was fictitious and that Leann was truly a stranger to M. They could confidently and accurately conclude that no s. 8 concern would arise from reviewing these communications. Section 8

jurisprudence is predicated on police obtaining prior authorization before a potential privacy breach. No such potential existed in this case. Section 184.2 of the *Criminal Code* does not apply in the instant case because a communication made under circumstances in which there is no reasonable expectation of privacy cannot constitute a "private communication" for the purposes of s. 183.

Per Wagner C.J. and **Karakatsanis** J.: There is agreement that the appeal should be dismissed, but for different reasons. When undercover police officers communicate in writing with individuals, there is no search or seizure within the meaning of s. 8 of the *Charter*. This is because an individual cannot reasonably expect their words to be kept private from the person with whom they are communicating. Here, the police did not interfere with a private conversation between other individuals; they directly participated in it. The police also did not violate s. 8 of the *Charter* when they communicated with M and retained screenshots of those conversations. Because the conversation occurred via email and Facebook, it necessarily took place in a written form. The screenshots from the screen capture software are simply a copy of the pre-existing written record and not a separate surreptitious permanent record created by the state.

Not every investigatory technique constitutes a search or seizure — s. 8 may be engaged only where the investigatory conduct intrudes upon a person's reasonable expectation of privacy. Section 8 does not prevent police from communicating with individuals in the course of an undercover investigation, because

the investigatory technique of engaging in conversation, even where the officer is undercover, does not diminish an individual's reasonable expectation of privacy. Here, an undercover police officer conversed with M using Facebook and email. This is no different from someone speaking to an undercover officer in person. M clearly intended for the recipient (who happened to be a police officer) to receive his messages. Because he had no reasonable expectation that his messages would be kept private from the intended recipient, s. 8 is not engaged.

The police's use of the screen capture software is also not a search or seizure. There is no relevant difference in the state preserving the conversations by taking a screenshot of them rather than using a computer to print them or tendering a phone or laptop with the conversations open and visible. This use of technology is not intrusive or surreptitious state conduct. Furthermore, the permanent record of the conversation resulted from the medium through which M chose to communicate. He could not reasonably expect that the intended recipient of his communications would not have a written record of his words. Because the police techniques used in the instant case did not engage the protections of s. 8, judicial pre-authorization was not required.

While the Internet empowers individuals to exchange much socially valuable information, it also creates more opportunities to commit crimes. Undercover police operations, using the anonymity of the Internet, allow police officers to proactively prevent sexual predators from preying on children.

Per **Moldaver** J.: The reasons provided by Karakatsanis J. and Brown J. are sound in law and each forms a proper basis for dismissing the appeal.

Per **Martin** J.: The state surveillance of M's private communications constituted a search that breached s. 8 of the *Charter*. It was objectively reasonable for M to expect that a permanent recording of the communications between himself and the police officer would not be surreptitiously acquired by an agent of the state absent prior judicial authorization. The police officer's use of the screen capture software constituted an "interception" within the meaning of Part VI of the *Criminal Code*. Because he did not obtain prior judicial authorization, the search was unreasonable. However, the application to exclude the evidence pursuant to s. 24(2) of the *Charter* was properly dismissed. While the impact of the breach was significant, the seriousness of the breach was minimal. Exclusion of relevant and reliable evidence in a child-luring case, obtained using tactics that the police had good reason to believe were legal at the time of the investigation, would bring the administration of justice into disrepute.

The regulation of an ever-changing internet requires careful balancing of rights and interests. The sexual exploitation of a minor is an abhorrent act and children and youth are particularly vulnerable on the internet. State actors must be equipped with investigative powers that will allow them to root out sexual exploitation online. Such investigative powers, however, need to be counter-balanced with the state's obligation to respect the privacy rights of its citizens. Reasonable

expectation of privacy is assessed on a normative, rather than descriptive, standard. The question to be asked is whether the privacy claim must be recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society. In a free and democratic society, it is reasonable to expect that the state will only access electronic recordings of private communications if it has sought authorization to do so.

R. v. Duarte, [1990] 1 S.C.R. 30, held that surreptitious participant electronic surveillance by the state requires regulation. Warrantless surveillance at the sole discretion of the police annihilates the right of individuals to choose the range of their auditors and imposes a risk of having to contend with a documented record of their words. This effectively strips freedom of thought and expression of any meaning. In response to *Duarte*, Parliament enacted s. 184.2 of the *Criminal Code* which requires prior judicial authorization for electronic state participant surveillance. In *Duarte*, documentation of private communications occurred via state recording technology. Now, individuals communicate using electronic media, such that their conversations are inherently recorded, and the way to obtain a real-time record of a conversation is simply to engage in that conversation. This shift in communication methods should not mean that the state should no longer be required to seek authorization to access electronic recordings of private communications. Otherwise, there would be no meaningful residuum to the right to live free from surveillance.

The electronic communications in the case at bar are a hybrid of an oral conversation and the surreptitious electronic recording of that conversation that attracted a reasonable expectation of privacy in *Duarte*. 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. Contemporary electronic communications are analogous to electronic recordings because they possess the characteristics of permanence, evidentiary reliability, and transmissibility that define electronic recordings and they are a documented record of the conversation. That conversants are aware that their communications are being recorded and knowingly create the record does not mean that electronic communications must be analogized to oral conversations nor does it destroy any reasonable expectation of privacy. Creating written, electronic records of one's private communications is a virtual prerequisite to participation in modern society, yet individuals still retain subjective and objective expectations of privacy in those communications. Unregulated state electronic surveillance will lead to self-censoring online and will annihilate society's sense of privacy.

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. In the case of state participant surveillance, the notion of intended recipient is infused with the concept of the right to choose one's listeners. An individual retains the reasonable expectation that the state will only permanently record a private communication with judicial

authorization. Further, there are quantitative and qualitative distinctions between in-person and electronic state surveillance that make the analogy between the "conversations" in *Duarte* and today's electronic communications untenable. Quantitatively, in-person conversations with undercover police officers are not capable of subjecting the public to surreptitious electronic surveillance on a mass scale due to the practical resource constraints of undercover police work whereas electronic surveillance technologies make possible mass surveillance as never before. Qualitatively, the ability to fabricate alternative identities has never been more possible and on-line anonymity allows for a different order of state surveillance using believable, false identities. Finally, state action that intrudes on a reasonable expectation of privacy is intended to be addressed via s. 8 of the *Charter*. Placing communications outside s. 8 because the state recipient can obtain a record simply by engaging in the conversation undermines the purpose of privacy rights and upsets the careful balance between the ability of the state to investigate crime and the rights of individuals to private areas of expression.

Determining whether there is a reasonable expectation of privacy based on a category of relationship is risk analysis reasoning, not content neutral, and puts courts in the business of evaluating personal relationships with a view to deciding which deserve *Charter* protection under s. 8, and which do not. Judicial disapprobation of an accused's lifestyle has no place in the s. 8 privacy analysis. Finally, a finding of reasonable expectation of privacy does not mean that the state is forbidden from conducting a search — it means that the police action must be

supported by a power that respects s. 8 of the *Charter*. The scenario presented of a sting context in which the state pretends to be a child and communicates with those seeking to sexualize children is the type of circumstance in which the state could and should obtain judicial authorization to surveil private, electronic communications. The risk that one's co-conversant may disclose a private communication does not affect the reasonableness of the expectation that the state, in the absence of such disclosure, will not intrude upon that private communication. Under s. 8, the analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought. It is not reasonable to assume that communications between adults and children who do not know each other will be criminal in nature. Content neutrality was developed to ensure that unjustified state intrusions into privacy would not occur. The s. 8 inquiry has never assumed that some relationships are *a priori* criminal and therefore do not legitimately attract an expectation of privacy. It is not the role of the courts to evaluate personal relationships with a view to denying s. 8 *Charter* protection to certain classes of people.

The use of screen capture software fits within the definitions of "intercept" and "private communication" under s. 183 of the *Criminal Code*. The word "intercept" denotes an interference between the sender and recipient in the course of the communication process. The police officer recorded the informational content of the private communications when he saved them for the sake of reproduction for the courts in real-time. Applying Part VI in this case strikes the right

balance between law enforcement's need to investigate crime and the right to be left alone. Even in the absence of screen capture software, it may be that the state investigative technique employed here constituted an "interception". In communicating with M over a medium that inherently produces an electronic recording, the police officer "acquired" a record of the communication. If electronic police surveillance of private communications is only regulated by Part VI to the extent that extraneous recording software is employed, it is no longer sufficiently comprehensive. To be constitutionally compliant, state acquisition in real-time of private electronic communications requires regulation.

Cases Cited

By Brown J.

Distinguished: *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Duarte*, [1990] 1 S.C.R. 30; **referred to:** *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Edwards*, [1996] 1 S.C.R. 128; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696; *R. v. Graff*, 2015 ABQB 415, 337 C.R.R. (2d) 77; *R. v. Ghotra*, [2015] O.J. No. 7253; *R. v. George*, 2017 SCC 38, [2017] 1 S.C.R. 1021; *R. v. Morrison*, 2019 SCC 15; *R. v. K.R.J.*, 2016 SCC 31, [2016] 1 S.C.R. 906; *R. v.*

Budreo (2000), 46 O.R. 481; *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3.

By Karakatsanis J.

Considered: *R. v. Duarte*, [1990] 1 S.C.R. 30; **referred to:** *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Fearon*, 2014 SCC 77, [2014] 3 S.C.R. 621; *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Levigne*, 2010 SCC 25, [2010] 2 S.C.R. 3; *R. v. Evans*, [1996] 1 S.C.R. 8; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, 40 C.R. (7th) 379; *R. v. Fliss*, 2002 SCC 16, [2002] 1 S.C.R. 535; *R. v. Oickle*, 2000 SCC 38, [2000] 2 S.C.R. 3; *Rothman v. The Queen*, [1981] 1 S.C.R. 640; *R. v. Mack*, [1988] 2 S.C.R. 903; *R. v. Hart*, 2014 SCC 52, [2014] 2 S.C.R. 544; *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696; *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Alicandro*, 2009 ONCA 133, 95 O.R. (3d) 173; *R. v. Legare*, 2009 SCC 56, [2009] 3 S.C.R. 551; *R. v. Chiang*, 2012 BCCA 85, 286 C.C.C. (3d) 564; *R. v. Bayat*, 2011 ONCA 778, 108 O.R. (3d) 420; *R. v. Babos*, 2014 SCC 16, [2014] 1 S.C.R. 309.

By Martin J.

Considered: *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; **referred to:** *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Patrick*, 2009 SCC 17, [2009]

1 S.C.R. 579; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Reeves*, 2018 SCC 56; *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 320; *R. v. Wong*, [1990] 3 S.C.R. 36; *United States v. White*, 401 U.S. 745 (1971); *R. v. Pires*, 2005 SCC 66, [2005] 3 S.C.R. 343; *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696; *R. v. Fliss*, 2002 SCC 16, [2002] 1 S.C.R. 535; *Holmes v. Burr*, 486 F.2d 55 (1973); *R. v. Wise*, [1992] 1 S.C.R. 527; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *Rothman v. The Queen*, [1981] 1 S.C.R. 640; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211; *R. v. Craig*, 2016 BCCA 154, 335 C.C.C. (3d) 28; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569; *R. v. Fearon*, 2014 SCC 77, [2014] 3 S.C.R. 621; *R. v. Belnavis*, [1997] 3 S.C.R. 341; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Collins*, [1987] 1 S.C.R. 265; *R. v. Kwok*, [2008] O.J. No. 2414; *R. v. Blais*, 2017 QCCA 1774, *R. v. Beairsto*, 2018 ABCA 118, 359 C.C.C. (3d) 376; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27; *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Levigne*, 2010 SCC 25, [2010] 2 S.C.R. 3; *R. v. Plant*, [1993] 3 S.C.R. 281.

Statutes and Regulations Cited

Canadian Charter of Rights and Freedoms, ss. 8, 24(2).

Criminal Code, R.S.C. 1985, c. C-46, Part VI, ss. 172.1, 183 "intercept", "private communication", 184.2.

Authors Cited

Fitch, Gregory J. "Child Luring" in *Substantive Criminal Law, Advocacy and the Administration of Justice*, vol. 1, presented to the National Criminal Law Program. Edmonton: Federation of Law Societies of Canada, 2007.

Haggerty, Kevin D. "Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance" (2009), 17 *Critical Crim.* 277.

Hutchison, Scott C., et al. *Search and Seizure Law in Canada*. Toronto: Carswell, 1991 (loose-leaf updated 2018, release 7).

Lyon, David. *Surveillance After Snowden*. Cambridge: Polity Press, 2015.

MacFarlane, Bruce A., Robert J. Frater and Croft Michaelson. *Drug Offences in Canada*, vol. 2, 4th ed. Toronto: Thomson Reuters, 2015 (loose-leaf updated April 2017, release 2).

Marthews Alex, and Catherine Tucker, "The Impact of Online Surveillance on Behavior" in David Gray and Stephen E. Henderson, eds., *The Cambridge Handbook of Surveillance Law*. Cambridge: Cambridge University Press, 2017.

Penney, Jonathon W. "Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017), 6:2 *Internet Policy Review* 22 (online: https://policyreview.info/node/692/pdf; archived version: http://www.scc-csc.ca/cso-dce/2019SCC-CSC22_1_eng.pdf).

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

Penney, Steven, Vincenzo Rondinelli and James Stribopoulos. *Criminal Procedure in Canada*, 2nd ed. Toronto: LexisNexis, 2018.

Pomerance, Renee M. "Flirting with Frankenstein: The Battle Between Privacy and Our Technological Monsters" (2016), 20 *Can. Crim. L. Rev.* 149.

Stewart, Hamish. "Normative Foundations for Reasonable Expectations of Privacy" (2011), 54 *S.C.L.R.* (2d) 335.

Westin, Alan. *Privacy and Freedom*. New York: Ig Publishing, 1967.

APPEAL from a judgment of the Newfoundland and Labrador Court of Appeal (Welsh, Harrington and Hoegg JJ.A.), 2017 NLCA 12, [2017] N.J. No. 55 (QL), 2017 CarswellNfld 58 (WL Can.), affirming the conviction entered by Orr J.,

364 Nfld. & P.E.I.R. 237, 1136 A.P.R. 237, 332 C.R.R. (2d) 50, [2015] N.J. No. 97 (QL), 2015 CarswellNfld 79 (WL Can.). Appeal dismissed.

Rosellen Sullivan and *Michael Crystal*, for the appellant.

Lloyd M. Strickland and *Sheldon B. Steeves*, for the respondent.

Nicholas E. Devlin and *Amber Pashuk*, for the intervener the Director of Public Prosecutions.

Susan Magotiaux and *Katie Doherty*, for the intervener the Attorney General of Ontario.

Nicolas Abran and *Ann Ellefsen-Tremblay*, for the intervener Director of Criminal and Penal Prosecutions.

Daniel M. Scanlan, for the intervener the Attorney General of British Columbia.

Christine Rideout, for the intervener the Attorney General of Alberta.

Jill R. Presser and *Kate Robertson*, for the intervener Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

Frank Addario and *James Foy*, for the intervener Canadian Civil Liberties Association.

Gerald Chan and *Annamaria Enenajor*, for the intervener Criminal Lawyers' Association.

Rachel Huntsman, Q.C., for the intervener Canadian Association of Chiefs of Police.

The judgment of Abella, Gascon and Brown JJ. was delivered by

BROWN J. —

I. Introduction

[1] This appeal presents two issues: (1) whether the investigative technique employed by an undercover police officer amounted to a search or seizure of the appellant Sean Patrick Mills' online communications under s. 8 of the *Canadian Charter of Rights and Freedoms*; and, (2) whether police intercepted a private communication pursuant to s. 184.2 of the *Criminal Code*, R.S.C. 1985, c. C-46, absent prior judicial authorization.

[2] These issues arise from a sting conducted by a police officer, who posed online as a 14-year-old girl, with the intent of catching Internet child lurers. Over two months, Mills sent several messages, using Facebook and Hotmail. Eventually, he was arrested in a public park where he had arranged a meeting with the "child", and was charged under s. 172.1 of the *Criminal Code* with luring a child via the Internet. The entire operation occurred without prior judicial authorization.

[3] Using a screen capture software, the police introduced a record of the emails and messages as evidence at trial. Mills, arguing that his s. 8 *Charter* right to be free from unreasonable search and seizure was infringed, applied for the exclusion of the evidence. The trial judge, while finding that judicial authorization was required from the point at which the police had determined that Mills had a "potentially inappropriate interest" in a minor, nonetheless admitted the evidence and convicted Mills on one of the counts. The Newfoundland and Labrador Court of Appeal upheld his conviction, but found that Mills' expectation of privacy was not objectively reasonable.

[4] While I agree with the Court of Appeal that Mills had no reasonable expectation of privacy, I adopt slightly different reasons. Specifically, he could not claim an expectation of privacy that was objectively reasonable in these circumstances. He was communicating with someone he believed to be a child, who was a stranger to him, and the undercover officer knew this when he created her.

Therefore, since s. 8 of the *Charter* is not engaged, it follows that the sting did not require prior judicial authorization. I would therefore dismiss the appeal.

II. Overview of Facts and Proceedings

A. *Background*

[5] In February 2012, Constable Greg Hobbs of the Royal Newfoundland Constabulary created a Hotmail email account in order to pose as a 14-year-old girl, "Leann Power". Shortly thereafter, he created a Facebook profile under the same name, listing Leann's hometown as St. John's and identifying her high school. One month later, Mills (then 32 years old) contacted "Leann" through Facebook, pretending to be 23 years old. Over the next two months, he sent her several messages and emails, including a photo of his penis.

[6] The police maintained a record of the online communications and emails, through a screen capture software called "Snagit".

[7] On May 22, 2012, Mills was arrested in a park where he had arranged a meeting with Leann. He was charged with child luring under s. 172.1 of the *Criminal Code*. At trial, he argued that the police, which operated the sting entirely without judicial authorization, ought to have obtained authorization under s. 184.2 of the *Criminal Code*, and that the search and seizure (by Snagit) of the communications

obtained via the fake online profile breached his s. 8 *Charter* right. He therefore applied to exclude the evidence.

B. *Judicial History*

(1) Newfoundland and Labrador Provincial Court — Orr Prov. Ct. J. ((2013), 7 C.R. (7th) 268)

[8] The trial judge found that the messages were "private communications", as defined in s. 183 of the *Criminal Code*. Because the police were party to those communications, their interception was subject to the requirements of s. 184.2 ("Interception with consent"). While Facebook and Hotmail automatically generated a record of the communications, the use of Snagit generated an additional seizure. And, because Mills was using a username and a password, he had an expectation of privacy in his communications — which, while perhaps *limited* by the recipient's use of an alias or false identity, was not *eliminated*.

[9] The judge therefore found that s. 8 of the *Charter* was breached. Judicial authorization was required from the point that Cst. Hobbs became aware of Mills' "potentially inappropriate interest" in Leann.

[10] In separate reasons on the admissibility under s. 24(2) of the *Charter* of the communications, the trial judge found that admitting the evidence would not bring

the administration of justice into disrepute (*R. v. Mills* (2014), 346 Nfld. & P.E.I.R. 102), and convicted Mills.

(2) Newfoundland and Labrador Court of Appeal — Welsh, Harrington and Hoegg JJ.A. (2017 NLCA 12)

[11] While the Court of Appeal upheld Mills' conviction, it reasoned that there was no "interception" and that the trial judge had therefore erred in concluding that authorizations under s. 184.2 were required. Relying on the factors set out in *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212 (at para. 18) by which to assess the reasonable expectation of privacy of an individual, the court found (at para. 23) that Mills must have known that "he lost control over any expectation of confidentiality [and] took a risk when he voluntarily communicated with someone he did not know". In the result, his expectation of privacy was not objectively reasonable and his s. 8 rights were not infringed.

III. Analysis

A. *Section 8 Charter Analysis: Mills Has no Reasonable Expectation of Privacy*

[12] In *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, this Court reiterated that, to claim s. 8's protection, an accused must show a subjectively held, and objectively reasonable, expectation of privacy in the subject matter of the putative search: para. 10; see also *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at

para. 34; *Spencer*, at para. 16; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 18; *R. v. Edwards*, [1996] 1 S.C.R. 128, at para. 45; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 159-60. I say "putative search", since there is no "search and seizure" within the meaning of s. 8 if the claimant cannot demonstrate a reasonable expectation of privacy: *R. v. Dyment*, [1988] 2 S.C.R. 417, at p. 426; see also S. Penney, V. Rondinelli and J. Stribopoulos, *Criminal Procedure in Canada* (2d ed. 2018), at pp. 151-52; H. Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011), 54 *S.C.L.R.* (2d) 335, at p. 335.

[13] Objective reasonableness is assessed in the "totality of the circumstances": *Edwards*, at paras. 31 and 45; *Marakah*, para. 10; *Spencer*, at paras. 16-18; *Cole*, at para. 39; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 26; *Tessling*, at para. 19. And, this Court has also consistently maintained that examining the totality of the circumstances entails an evaluation of all aspects of privacy: *Edwards*, at para. 45; *Patrick*, at para. 26. Four lines of inquiry guide the application of the test: (1) an examination of the subject matter of the alleged search; (2) a determination as to whether the claimant had a direct interest in the subject matter; (3) an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and (4) an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances: *Cole*, at para. 40; *Marakah*, at para. 11; *Spencer*, at para. 18; *Patrick*, at para. 27; *Tessling*, at para. 32.

(1) What Was the Subject Matter of the Alleged Search?

[14] The subject matter of the alleged search is the electronic communications that took place on Facebook "chat" and over email. I see no legally significant distinction between these media of communication and the text message exchanges on cellphones which this Court considered in *Marakah*. Each can be accessed via many electronic devices connected to the Internet. And, in *Marakah*, this Court refused to distinguish among different messaging applications, since they are functionally equivalent as an "interconnected system . . . [which] . . . functions to permit rapid communication of short messages between individuals" — which exchanges, the Court added, is the very thing that law enforcement seeks to access: *Marakah*, at paras. 18-19.

[15] While in this case police were the direct recipients of Mills' messages, it remains that he intended to have a one-on-one online conversation. This tends to support recognizing an expectation of privacy in those communications.

(2) Did Mills Have a Direct Interest in the Subject Matter?

[16] I accept that, as a participant to (and indeed a co-author of) the communications, Mills had a direct interest in the subject matter of the alleged search: see *Marakah*, at para. 21; *Spencer*, at para. 50; *Patrick*, at para. 31.

(3) Did Mills Have a Subjective Expectation of Privacy in the Subject Matter?

[17] In cases of alleged online child luring, it is not difficult for an accused to demonstrate a subjective expectation of privacy in online communications, since avoiding detection will be a priority. Users expect that their text messages or (as here) their functional equivalent will remain private: *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696, at para. 34. And so it is unsurprising that, here, the Crown does not dispute that Mills expected the communications to be private.

[18] The evidence amply demonstrates this, since Mills instructed Leann to delete their messages regularly and to empty her deleted messages folder. When Leann commented on a publication he had posted on Facebook, he deleted it immediately then privately messaged her to explain that his mother was also a Facebook user and that he would "just rather not hear what she has to say about our age difference": A.R., vol. 2, at p. 86. Replying to an email in which Cst. Hobbs had sent Mills pictures supposedly portraying Leann, Mills promised to keep their relationship secret. He added that he expected the same from her: A.R., vol. 2, at p. 122. Similarly, when Mills sent a picture of his erect penis to Leann, he instructed her to delete all of their conversations. He wrote: "can't be too careful and I'd say you would get in trouble with pics like this". The title of the email, "delete this after you look at it!!", also shows his wish that their relationship remain hidden: A.R., vol. 2, at p. 135.

[19] This consideration therefore also weighs in favour of Mills' claim to a reasonable expectation of privacy. It remains to consider, however, whether his subjective expectation of privacy was objectively reasonable: B. A. MacFarlane, R. J. Frater and C. Michaelson, *Drug Offences in Canada* (4th ed. (loose-leaf)), vol. 2, at p. 24-15.

(4) Is Mills' Subjective Expectation of Privacy Objectively Reasonable?

[20] In order to challenge an alleged search under s. 8, Mills must demonstrate the objective reasonableness of his claim to privacy — the assessment of which must have regard to the totality of the circumstances. This is not purely a descriptive question, but rather a normative question about when Canadians *ought* to expect privacy, given the applicable considerations. This appeal involves a particular set of circumstances — the police created one of the communicants and controlled her every move — and two considerations become decisive: the nature of the investigative technique used by police, and the nature of the relationship between the communicants. Specifically, here, the investigative technique did not significantly reduce the sphere of privacy enjoyed by Canadians because the technique permitted the state to know from the outset that the adult accused would be communicating with a child he did not know. As I will explain, in these circumstances, any subjective expectation of privacy the adult accused might have held would not be objectively reasonable.

[21] Before turning to the normative question, as a preliminary matter, the nature of the privacy interest must be determined. Here, Mills asserts an informational privacy interest. As this Court held in *Spencer*, informational privacy includes at least three conceptually distinct although overlapping understandings of privacy: as *secrecy*, as *control*, and as *anonymity*: para. 38. Mills is asserting a "privacy as control" interest in the content of his communications, which represents the "assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit": *Spencer*, at para. 40. While this privacy interest protects what information we share with others, it in turn relies on the control that a person exercises by choosing, *selectively*, those particular persons who will receive this information. In effect, Mills argues that he chose his recipient (here, someone he believed to be a child who was a stranger to him), and the police's creation of a fake online profile prevented him being able to converse in secret with the person he chose.

[22] But crucial here is that Mills was communicating with someone he believed to be a *child*, who was a *stranger* to him. Mills' claim is, therefore, that even when conversing with a child who was a stranger to him, he retained the ability to choose, *selectively*, with whom he would share certain communications. This presupposes that there is nothing inherently different between a relationship involving an adult and a child unknown to them, and other relationships, for the purposes of the s. 8 privacy analysis. I disagree and, on this point, find the statements of Nielsen J. in *R. v. Graff*, 2015 ABQB 415, 337 C.R.R. (2d) 77, at paras. 63 and 65, where the

accused was charged with internet luring of a recipient who identified as being 14 years old, to be apposite:

> In sum, the applicant sent highly personal information over the internet to a complete stranger, in the absence of any invitation to send such information, and without taking any reasonable steps to ascertain the identity of the recipient, to ensure his own anonymity, or to ensure any confidentiality with respect to the information he sent.
>
> . . .
>
> I conclude in all of the circumstances that while the applicant gambled or hoped that the chat and other material and information he sent would remain private, he had no basis upon which to form a[n] . . . objectively reasonable expectation of privacy in the circumstances.

See also *R. v. Ghotra*, [2015] O.J. No. 7253 (Q.L.) (S.C.J.), at para. 128.

[23] This Court has recognized that children are especially vulnerable to sexual crimes (*R. v. George*, 2017 SCC 38, [2017] 1 S.C.R. 1021, at para. 2); that the Internet allows for greater opportunities to sexually exploit children (*R. v. Morrison*, 2019 SCC 15, at para. 2); and that enhancing protection to children from becoming victims of sexual offences is vital in a free and democratic society (*R. v. K.R.J.*, 2016 SCC 31, [2016] 1 S.C.R. 906, at para. 66, citing Laskin J.A. in *R. v. Budreo* (2000), 46 O.R. 481 (C.A.)). This leads me to conclude that, on the normative standard of expectations of privacy described by this Court (*Tessling*, at para. 42), adults cannot reasonably expect privacy online with children they do not know. That the communication occurs online does not add a layer of privacy, but rather a layer of unpredictability.

[24] The difficulty, of course, is that, in most situations, police are unlikely to know in advance of any potential privacy breach the nature of the relationship between the conversants — for example, whether the child truly is a stranger to the adult. We must also bear in mind that most relationships between adults and children are worthy of s. 8's protection, including, but in no way limited to, those with family, friends, professionals, or religious advisors. Significantly, *and most importantly for the disposition of this appeal*, this difficulty does not arise here. Here, the police were using an investigative technique allowing it to *know from the outset* that the adult was conversing with a child who was a stranger. Different normative considerations arise here, both as to the nature of the relationship and how that informs the s. 8 analysis, and as to the degree by which the investigative technique reduces the sphere of privacy enjoyed by Canadians.

[25] While this Court has not traditionally approached s. 8 from the perspective of the particular relationship between the parties subject to state surveillance, this is because of its view of s. 8's protection as content-neutral. In this case, the police technique permitted them to know that relationship in advance of any potential privacy breach. For example, in *Dyment*, the majority of the Court held that, while a person may consent to give a sample of blood requested by his or her physician, it does not follow that all privacy interests in the sample have been relinquished once the blood has left the person's body. The 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. The Court wrote, at para. 28:

"the *Charter* extends to prevent a police officer . . . from taking . . . blood from a person who holds it subject to a duty to respect the dignity and privacy of that person" (emphasis added). While, therefore, the patient had relinquished *physical* control over the sample, he was able — by reason of the privacy interest imbued in the *relationship* — to retain *legal* control over it.

[26] In short, the sample was a proxy for s. 8's purpose in *Dyment*, being to protect a particular relationship — which society values as worthy of s. 8's protection — from state intrusion. Applied to this appeal, and while I have said that many adult-child relationships are also worthy of s. 8's protection — the relationship between Mills and "Leann" is not one of them, if expectations of privacy are to reflect a normative (rather than a purely descriptive) standard. The conclusion may or may not apply to other types of relationships, depending on the nature of the relationship in question and the circumstances surrounding it at the time of the alleged search.

[27] As to the second consideration — the nature of the investigative technique used — what renders Mills' expectation of privacy objectively unreasonable is that, in creating the fictitious child, police knew from the outset that the relationship between Mills and his interlocutor was similarly fictitious, and that "Leann" was truly a stranger to him. The police could, therefore, confidently and accurately conclude that no s. 8 concern would arise from their reviewing these particular communications, because the necessary information about the nature of the relationship between the accused and the "child" was already known from the outset.

[28] Our s. 8 jurisprudence is predicated on police obtaining prior authorization before a *potential* privacy breach. But no such potential exists here. The police *created* the fictitious child and waited for adult strangers to message them. This is what distinguishes this case from *R. v. Wong*, [1990] 3 S.C.R. 36, and *Marakah*, where the state was intruding upon an unknown (to them) relationship. At most, police had a mere *theory* about the relationship between the conversants: in *Wong*, for example, they were thought to be illegal gamblers. It would only be through an examination of the conversation that the true nature of the relationship could have been definitively known. In contrast, police knew from the outset the nature of the relationship between these conversants. This also distinguishes this case from the impersonation-through-informer technique employed in *R. v. Duarte*, [1990] 1 S.C.R. 30.

[29] This investigative technique allowed the police to know from the outset the nature of the relationship between Mills and "Leann". As my colleague Karakatsanis J. notes, this technique involved police simply responding to messages sent directly to them as "Leann". No risk of potential privacy breach — for example, police sifting various communications before being able to ascertain the relationship — arose here.

[30] My colleague Martin J. says that these reasons "put 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, and which do not"

(para. 110) and "effectively sanctio[n] the unjustified state intrusion into swaths of all individuals' private lives in the hopes of capturing some illegal communications" (para. 131). With respect, the alias-based sting operation employed here is not some first step to a dystopian world of mass unregulated surveillance. Nothing in these reasons suggests or should be taken as suggesting that police can simply monitor communications in the hope of stumbling upon a conversation that reveals criminality. The proposition that I advance is a modest one: to repeat, it is that Mills cannot establish an objectively reasonable expectation of privacy in these particular circumstances, where he conversed with *a child* online who was *a stranger* to him and, *most importantly*, where the police knew this when they created her.

[31] With respect for those who view the matter differently, I simply cannot accept that, on the facts of this case, "giving [judicial] sanction to the particular form of unauthorized surveillance in question would see the amount of privacy and freedom remaining to citizens diminished to a compass inconsistent with the aims of a free and open society": *Wong*, at p. 46. I agree with the Court of Appeal's conclusion that Mills did not have a reasonable expectation of privacy in these circumstances.

B. *Additional Consideration*

[32] My conclusion on the unreasonableness of Mills' expectation of privacy is determinative. That said, I offer this further observation on whether Part VI of the

Criminal Code captured these communications because they consisted of "private communication".

[33] In my view, s. 184.2 of the *Criminal Code* was not applicable here because there was no "private communication". Section 184.2(1) states that "[a] person may intercept, . . . a private communication where either the originator of the private communication or the person intended by the originator to receive it has consented to the interception and an authorization has been obtained pursuant to subsection (3)". Section 183 defines "private communication" and "intercept" for the purpose of Part VI:

> **183** In this Part,
>
> . . .
>
> ***intercept*** includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;
>
> . . .
>
> ***private communication*** means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it;
>
> . . .

[34] Reading this definition together with this Court's elaboration of s. 8 of the *Charter*, a communication made under circumstances in which there is no reasonable expectation of privacy cannot constitute a "private communication" for the purposes of s. 183: *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3, at para. 32; S. Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap", (2018) 56 *Alta. L. Rev.* 1, at p. 18.

IV. Conclusion

[35] In the result, Mills has failed to establish that he had a reasonable expectation of privacy in his conversations with "Leann". I would, therefore, dismiss the appeal.

The reasons of Wagner C.J. and Karakatsanis J. were delivered by

KARAKATSANIS J. —

[36] I agree with my colleague Brown J. on the outcome of this appeal. However, I reach this conclusion for different reasons. In my view, when undercover police officers communicate in writing with individuals, there is no "search or seizure" within the meaning of s. 8 of the *Canadian Charter of Rights and Freedoms*. This is 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).

Further, the police conduct does not amount to a search or seizure — the police did not take anything from the accused or intrude on a private conversation; the undercover officers simply received messages sent directly to them.

[37] Here, the police did not interfere with a private conversation between other individuals; they directly participated in it. Because the conversation occurred via email and Facebook messenger, it necessarily took place in a written form. The screenshots from the computer program "Snagit" are simply a copy of the pre-existing written record and not a separate surreptitious permanent record created by the state. Thus, the police did not violate s. 8 when they communicated with Mr. Mills and retained screenshots of those conversations. I would dismiss the appeal.

I. Analysis

[38] Section 8 protects the right to be secure against unreasonable searches and seizures. In interpreting s. 8, courts seek to strike an acceptable balance, in a free and democratic society, between sometimes conflicting interests in the privacy necessary for personal dignity and autonomy and the need for a secure and safe society: see *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 159-60.

[39] The right to be secure against unreasonable searches and seizures must keep pace with technological developments to ensure that citizens remain protected against unauthorized intrusions upon their privacy by the state: *R. v. Fearon*, 2014 SCC 77, [2014] 3 S.C.R. 621, at para. 102; see also *R. v. Wong*, [1990] 3 S.C.R. 36, at

p. 44. However, as technology evolves, the ways in which crimes are committed — and investigated — also evolve. This case implicates both of these consequences. It requires us to consider what, if any, judicial pre-authorization is necessary when a common police investigative technique — an undercover operation — is conducted electronically to "identify and apprehend predatory adults who, generally for illicit sexual purposes, troll the Internet to attract and entice vulnerable children and adolescents": *R. v. Levigne*, 2010 SCC 25, [2010] 2 S.C.R. 3, at para. 24.

A. *Electronic Conversations in Undercover Police Investigations*

[40] In my opinion, no "search or seizure" occurred when Constable Hobbs, posing as a young girl, conversed with Mr. Mills through Facebook messenger and email.

[41] Not every investigatory technique used by the police constitutes a search or seizure for constitutional purposes — s. 8 may be engaged only where the investigatory conduct intrudes upon a person's reasonable expectation of privacy: *R. v. Evans*, [1996] 1 S.C.R. 8, at para. 11; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 18; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 34. As Doherty J.A. recognized, "[w]hen deciding whether state conduct amounts to a search or seizure, the focus is not so much on the nature of the state conduct as it is on the impact of the state conduct on the privacy interests of the s. 8 claimant": *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, 40 C.R. (7th) 379, at para. 39.

[42] This Court has long recognized that s. 8 does not prevent police from communicating with individuals in the course of an undercover investigation. This is because an individual cannot reasonably expect their words to be kept private from the person with whom they are communicating. Section 8 does not apply because the investigatory technique of engaging in conversation, even where the officer is undercover, does not diminish an individual's reasonable expectation of privacy. Both *R. v. Duarte*, [1990] 1 S.C.R. 30, and *R. v. Fliss*, 2002 SCC 16, [2002] 1 S.C.R. 535, involved conversations between undercover police officers and the accused. In neither case did the conversation itself engage s. 8. As La Forest J. wrote in *Duarte*, at p. 57, "[a] conversation with an informer does not amount to a search and seizure within the meaning of the *Charter*. Surreptitious electronic interception and recording of a private communication does" (emphasis added). In her concurring reasons in *Fliss*, at para. 12, Arbour J. echoed this point, holding that "a conversation with an informer, or a police officer, is not a search and seizure. Only the recording of such conversation is."

[43] Similarly, undercover police investigations have long been recognized as legitimate and important law enforcement tools. Police do not need to obtain judicial pre-authorization before beginning an undercover investigation. This Court has acknowledged that police may employ creativity and subterfuge in their work of preventing and investigating crime, although the police conduct must not threaten the integrity of the criminal justice system: see *R. v. Oickle*, 2000 SCC 38, [2000] 2 S.C.R. 3, at paras. 65-67, citing *Rothman v. The Queen*, [1981] 1 S.C.R. 640, at p.

697 (per Lamer J. (as he then was), concurring); *R. v. Mack*, [1988] 2 S.C.R. 903, at pp. 916-17; *R. v. Hart*, 2014 SCC 52, [2014] 2 S.C.R. 544, at para. 83.

[44] Here, an undercover police officer conversed with Mr. Mills using Facebook messenger and email. Obviously, Mills did not realize he was talking to someone who was an undercover officer. However, this is no different from someone who unwittingly speaks to an undercover officer in person. *Fliss* makes clear that individuals conversing orally with an undercover officer are not thereby subject to a search or seizure within the meaning of the *Charter*, even if they have no reason to believe they are speaking to the police. In this case, Mr. Mills clearly intended for the recipient (who happened to be a police officer) to receive his messages. It would not be reasonable for him to expect otherwise. Because he had no reasonable expectation that his messages would be kept private from the intended recipient, s. 8 is not engaged.

[45] The fact that the conversation took place in a written form, rather than orally as in *Duarte* and *Fliss*, does not transform it into a search or seizure. For example, 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.

[46] The appellant submits that the combined effect of *Duarte* and *Wong* requires the police to always obtain prior judicial authorization before engaging in individual undercover conversations online. In his view, the police conduct in this case is "indistinguishable" from the surreptitious recording in *Duarte*.

[47] However, the common thread between *Duarte* and *Wong* was not the use of undercover officers, but the state's unilateral decision to make surreptitious audio and video recordings of oral conversations. This prospect was troubling because the police transformed an ephemeral oral conversation into a permanent record without the knowledge of the person who was speaking. The issue was whether the state's newfound technological ability to "listen in" on conversations should require judicial pre-authorization. And with respect to the prospect of surreptitious audio and video recordings of our everyday lives, the Court concluded that the threat to individual freedom and autonomy outweighed the state's valid law enforcement objectives.

[48] But in this case, Mr. Mills chose to use a written medium to communicate with Constable Hobbs. Email and Facebook messenger users are not only aware that a permanent written record of their communication exists, they actually create the record themselves. The analogy with *Duarte* is to the oral conversation, not the surreptitious recording of that conversation. *Duarte* did not deal with a written record created by an individual communicating with an undercover officer. As such, it does not require the police to obtain a warrant before using modern communication methods such as text messages or emails during undercover investigations.

[49] My colleague Martin J. raises the spectre of "surreptitious electronic surveillance on a mass scale": para. 103. However, the investigatory technique in this case involved a one-on-one conversation between an undercover officer and the accused. This Court has held that generally, police attempts to obtain written,

electronic conversations are subject to s. 8. Police are required to obtain a warrant before accessing text message conversations stored by telecommunications providers: *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696, at paras. 77-81; *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3, at paras. 12-13 and 48-49. Similarly, viewing a text message conversation between two other parties, without their consent, also engages s. 8 of the *Charter*: *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, at paras. 54-57.

[50] This approach does not re-introduce the "risk analysis" rejected in *Duarte*. Section 8 protects "the expectation that our words will only be heard by the person or persons to whom we direct our remarks": *Duarte*, at p. 47. In this case, that is precisely what occurred — Mills' communications were received by their intended recipient, who happened to be a police officer. By communicating online with a person he had never met before, Mills opened himself up to the possibility that the other person was a police officer. The *Charter* cannot be invoked "to protect us against a poor choice of friends": *Duarte*, at p. 57.

[51] Thus, s. 8 of the *Charter* is not engaged merely because an undercover officer converses electronically with an individual. This is because (1) it is not reasonable for the sender to expect that the messages will be kept private from the intended recipient (even if the recipient is an undercover officer); and (2) the police conduct of communicating with an individual does not amount to a search or seizure.

Either way, the outcome is the same — s. 8 is not violated when police simply communicate with an individual.

[52] The alternative conclusion would significantly and negatively impact police undercover operations, including those conducted electronically: see S. C. Hutchison et al., *Search and Seizure Law in Canada* (loose-leaf), at s. 4(c)(v)(B) (discussing whether a communication obtained by impersonation or mistake has been intercepted). I agree with the intervener Canadian Association of Chiefs of Police that requiring police officers to obtain judicial authorization, especially Part VI authorization, prior to engaging in this type of undercover operation would "effectively hamstring the ability of the police to proactively enforce [child luring offences]": I. F., at para. 5. Particularly in a case like this, where there is no suspect before the investigation commences, police would not have grounds to obtain a warrant or Part VI authorization. As courts have recognized, undercover police operations are an important tool in enforcing the child luring offences and protecting vulnerable children: *Levigne*, at para. 25; *R. v. Alicandro*, 2009 ONCA 133, 95 O.R. (3d) 173, at para. 38. Requiring police to obtain judicial pre-authorization before even launching an electronic undercover investigation simply does not strike an appropriate balance between individual privacy and the safety and security of our children.

B. *Using "Snagit" to Take Screenshots of an Electronic Conversation*

[53] Mills submits that by using "Snagit" to take screenshots of the electronic messages he exchanged with the undercover officer, the police further violated his s. 8 *Charter* rights.

[54] The question remains then as to whether the use of "Snagit" otherwise amounts to a search or seizure, requiring some form of judicial authorization. Of course, even if the Crown were not permitted to tender the printed screenshots as evidence, the Crown could still call the officer to testify about what the accused said and the written record could be used to refresh the officer's memory: *Duarte*, at pp. 58 and 60; *Fliss*, at paras. 7, 12 and 43-45. However, permanently preserving the accused's own words, in a complete and accurate format, gives the state compelling evidence against the accused. Does the state's use of screenshot technology intrude upon the accused's reasonable expectation of privacy such that it constitutes a search or seizure?

[55] In my opinion, it does not. As discussed above, the permanent record of the conversation resulted from the medium through which Mr. Mills chose to communicate. He cannot reasonably expect that the recipient would not have a written record of his words.

[56] For this reason, the police officer's use of "Snagit" is also not a search or seizure. I cannot see any relevant difference in the state preserving the conversations by using "Snagit" to take screenshots of them, by using a computer to print them, or by tendering into evidence a phone or laptop with the conversations open and visible.

Ultimately, the "Snagit" screenshots are just a copy of the written messages. This use of technology is not intrusive or surreptitious state conduct.

[57] My conclusion that s. 8 is not engaged in this case does not mean that undercover online police operations will *never* intrude on a reasonable expectation of privacy. As technology and the ways we communicate change, courts play an important role in ensuring that undercover police techniques do not unacceptably intrude on the privacy of Canadians. Particularly in the context of the digital world, it is important for courts to consider both the nature and the scale of an investigative technique in determining whether s. 8 is engaged. With respect to the concern about the prospect of broader surveillance made possible by technological advances, as Binnie J. observed in *Tessling*, "[w]hatever evolution occurs in future will have to be dealt with by the courts step by step. Concerns should be addressed as they truly arise": para. 55.

[58] Because the police techniques used here did not engage the protections of s. 8, judicial pre-authorization was not required. Therefore, it is unnecessary to consider whether any of the police techniques constituted an "intercept" as defined in Part VI of the *Criminal Code*, R.S.C. 1985, c. C-46.

II. Conclusion

[59] The ultimate normative issue under s. 8 is "whether, in light of the impact of an investigative technique on privacy interests, it is right that the state should be

able to use that technique without any legal authorization or judicial supervision": H. Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011), 54 *S.C.L.R.* (2d) 335, at p. 342. I acknowledge that the Court in *Duarte* did not anticipate the widespread use of electronic communication. I also recognize that many individuals engage in extensive, private online conversations with people they have not previously met in person. But, while the Internet empowers individuals to exchange much socially valuable information, it also creates more opportunities to commit crimes. The anonymity of the online world enables some predatory adults to gain the trust of vulnerable children and entice them into sexual activity: *R. v. Legare*, 2009 SCC 56, [2009] 3 S.C.R. 551, at para. 2; *Levigne*, at para. 25.

[60] Undercover police operations, using the anonymity of the Internet, allow police officers to proactively prevent sexual predators from preying on children. For decades, police officers have used undercover operations to investigate and prevent crimes. The fact that conversations with undercover officers now occur in written form on the Internet does not, in itself, violate s. 8 of the *Charter*. However, this conclusion in no way gives the police a broad license to engage in general online surveillance of private conversations. Both s. 8 of the *Charter*, as outlined in *TELUS*, *Marakah* and *Jones*, as well as the common law doctrines of abuse of process and entrapment place limits on the ways police can use electronic communications in the course of an investigation.

[61] Interveners in this case raised the concern about the extent to which the police are permitted to impersonate other individuals to further their undercover objectives. The intervener Criminal Lawyers' Association submits that not applying s. 8 in the present case opens the door to the police posing as internet therapy providers or even creating their own dating service in an effort to monitor the addictions or sexual preferences of Canadians: I. F., at paras. 4-5.

[62] These scenarios are far removed from the facts of this particular case, where the officer created a single Facebook profile and did not initiate contact with anyone. More importantly, I am not persuaded that either s. 8 of the *Charter* or Part VI of the *Criminal Code* would be the proper vehicles to address these concerns. The threat of rogue police undercover investigations is better characterized as a broader threat to the integrity of the justice system. As Lamer J. recognized in *Rothman*, certain undercover techniques, such as posing as a prison chaplain or a legal aid lawyer to elicit incriminating evidence, go too far and must be condemned by courts *because they threaten the integrity of the justice system itself*: pp. 696-97.

[63] If such cases arise, where police impersonation tactics offend society's notions of decency and fair play, courts should invoke existing common law mechanisms to regulate undercover police investigations, including those conducted online. The abuse of process doctrine guards against coercive police conduct, such as preying on an accused's vulnerabilities, which threatens trial fairness and the integrity of the justice system: *Hart*, at paras. 111-18. In addition, if police go beyond

providing an opportunity to commit an offence and actually induce its commission, the entrapment doctrine applies: *Mack*, at pp. 964-66. Indeed, courts have used the entrapment doctrine to scrutinize sting operations similar to the one used here: see *R. v. Chiang*, 2012 BCCA 85, 286 C.C.C. (3d) 564, at paras. 14-21; *R. v. Bayat*, 2011 ONCA 778, 108 O.R. (3d) 420, at paras. 15-23. In such circumstances, trial judges have "wide discretion to issue a remedy — including the exclusion of evidence or a stay of proceedings": *Hart*, at para. 113; see also *R. v. Babos*, 2014 SCC 16, [2014] 1 S.C.R. 309, at paras. 30-47 and 53-57.

[64] My conclusion that the *Charter* does not require judicial authorization before police participate in undercover online conversations of this kind also does not prevent Parliament from enacting legislation to regulate these operations. Indeed, given the prevalence of electronic communication and the prospect of increased police surveillance online, a legislative scheme could provide helpful guidance about the appropriate use and reporting of undercover police techniques to prevent and investigate online crime.

[65] In conclusion, there was no violation of s. 8 when the police communicated with Mills and used "Snagit" to preserve the written record of those conversations. The screenshots of the conversations were therefore admissible evidence. I would dismiss the appeal.

The following are the reasons delivered by

MOLDAVER J. —

[66] Although my colleagues Karakatsanis J. and Brown J. provide separate reasons for dismissing the appeal, in my view, each set of reasons is sound in law and each forms a proper basis for upholding the order of the Newfoundland and Labrador Court of Appeal dismissing Mr. Mills' appeal.

[67] Accordingly, I concur in the result and would likewise dismiss the appeal.

The following are the reasons delivered by

MARTIN J. —

I. Introduction

[68] The regulation of an ever-changing internet presents many challenges for lawmakers and courts and requires the careful balancing of rights and interests.

[69] 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.

[70] Parliament has addressed the unique risks posed by online sexual predation through, *inter alia*, s. 172.1 of the *Criminal Code*, R.S.C. 1985, c. C-46 ("Code"). As tools of crime grow more sophisticated, so must law enforcement techniques. State actors must be equipped with investigative powers that will allow them to effectively and proactively root out the sexual exploitation of children online.

[71] Such investigative powers, however, need to be counter-balanced with the state's obligation to respect the privacy rights of its citizens. Parliament has taken steps in this regard by legislating when the state must seek judicial authorization for accessing certain types of private communications: see Part VI of the *Criminal Code*, "Invasion of Privacy". However, the relevant provisions in Part VI were enacted before the widespread use of modern means of electronic communications, which have the capacity to generate a written record of conversations.

[72] This appeal asks whether the state should be permitted to conduct warrantless surveillance of private, electronic communications, or whether that state surveillance should be regulated. In my respectful view, protecting children from online sexual exploitation, while essential, does not require the *unregulated* state surveillance of the public's private electronic communications. For the reasons that follow, I conclude that members of society have a reasonable expectation that their private, electronic communications will not be acquired by the state at its sole

discretion. If the police wish to acquire a record of those communications, for the legitimate and vitally important purpose of preventing sexual crimes against young people, such investigative activities must be regulated. The precise nature of such regulation is best left to Parliament.

[73] Thus, while the state should be empowered to prevent sexual predators from targeting children and youth online, members of society must not, and need not, be subjected to the unregulated state surveillance of their private electronic communications in order for the state to achieve these aims.

II. Relevant Facts

[74] In 2012, members of the Royal Newfoundland Constabulary's Child Exploitation Unit, one of whom was Constable Hobbs, conducted a sting operation with the intent of catching internet child lurers. On February 28 and March 12, 2012, Cst. Hobbs created an email and a Facebook account for a fictitious 14 year old individual whom he called "Leann Power". Cst. Hobbs testified that he knew of no policy manuals to guide this type of investigation, and that his investigatory tactics were left to his discretion. On "Leann's" Facebook profile, Cst. Hobbs pretended that "Leann" resided in St. John's and was a student at a local high school. He obtained a photograph from the internet to use as "Leann's" profile picture. While Cst. Hobbs did not make any "friend" requests, he received and accepted "friend" requests that resulted from "Leann's" affiliation with the local high school: see (2013), 343 Nfld. & P.E.I.R. 128, at paras. 3-4 and 40 ("Decision Re s. 8").

[75] On March 20, 2012, Cst. Hobbs received a Facebook message from Mr. Mills. Over the next two months, Mr. Mills exchanged several Facebook messages and emails with "Leann". Ultimately, Mr. Mills was arrested in a public park where he had arranged to meet "Leann". He was charged with four counts of luring a child under s. 172.1 of the *Criminal Code*: Decision Re s. 8, at paras. 1 and 5-10.

III. Admissibility of the Electronic Communications Between Mr. Mills and "Leann"

[76] Mr. Mills challenged the admissibility of the electronic communications exchanged between himself and "Leann" on two grounds: first, that the police failed to comply with s. 184.2 of the *Code* by not obtaining authorization prior to intercepting private communications; and second, that the state action constituted an unreasonable search and seizure contrary to s. 8 of the *Charter*.

[77] My colleagues have found that Mr. Mills had no reasonable expectation of privacy in his communications with "Leann". Without a reasonable expectation of privacy, there was no search. Further, Brown J. concludes that s. 184.2 of the *Code* does not apply to the case at bar, while Karakatsanis J. finds it unnecessary to consider the question.

[78] Respectfully, I depart from these conclusions. Mr. Mills had a reasonable expectation of privacy in the impugned communications, and the state's surveillance of those private communications therefore constituted a search. Further, the police

use of "Snagit" screenshot software was regulated by s. 184.2 of the *Code*: Cst. Hobbs intercepted private communications when he used "Snagit" to record his communications with Mr. Mills in real-time. As such, he was required to obtain an authorization pursuant to s. 184.2. Because Cst. Hobbs did not do so, he breached Mr. Mills' s. 8 *Charter*-protected privacy right. Further, even if Cst. Hobbs had chosen not to employ extraneous screen recording software, his investigative technique may still have constituted an "interception" for the purposes of s. 184.2.

[79] However, the admission into evidence of the impugned communications would not bring the administration of justice into disrepute under s. 24(2) of the *Charter*. I would therefore dismiss the appeal.

IV. Reasonable Expectation of Privacy in Private Electronic Communications

[80] Reasonable expectation of privacy is assessed on a normative, rather than descriptive, standard: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 159-60; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 42; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 14; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at para. 18; *R. v. Reeves*, 2018 SCC 56, at para. 28. This means that the question to be asked is whether the privacy claim must "be recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society": *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 320, at para 87.

[81] When responding to this question in the context of this appeal, the starting point is this Court's decision in *R. v. Duarte*, [1990] 1 S.C.R. 30.

A. *The Case of Duarte Is the Starting Point*

[82] As early as thirty years ago, this Court held that surreptitious participant electronic surveillance by the state requires regulation: *Duarte*, and its companion case, *R. v. Wong*, [1990] 3 S.C.R. 36. In *Duarte*, a group conversation about a cocaine transaction was surreptitiously recorded with the consent of two of the parties to the conversation – an informer and an undercover police officer. When a participant in a conversation either surreptitiously records that conversation or consents to the conversation being surreptitiously recorded, it is called "participant surveillance". At the time, s. 178.11(2)(a) of the *Code* permitted parties to a conversation to conduct electronic participant surveillance without a warrant. On the strength of a normative privacy analysis, La Forest J. held that the risk of warrantless surveillance at the sole discretion of the police cannot be imposed on all members of society. He further held that this principle applies equally in the case of participant surveillance. As such, warrantless electronic participant surveillance by the state infringes s. 8 of the *Charter*.

[83] At its core, surreptitious electronic recording of private communications by the state attracted a privacy interest in *Duarte* because recording a communication transforms the originator's ephemeral words into documentary evidence. The act of recording, therefore, "annihilates the very important right . . . to choose the range of

our auditors" (p. 51).This concern was expressed by Harlan J., dissenting in *United States v. White*, 401 U.S. (1971), at pp. 787-89 and referenced in *Duarte*, at p. 54, as "having to contend with a documented record". The risk of documentation and permanence is evoked in two of *Duarte*'s foremost statements of principle:

> the regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words (at p. 44, emphasis added); and
>
> the law recognizes that we inherently have to bear the risk of the 'tattletale' but draws the line at concluding that we must also bear, as the price of choosing to speak to another human being, the risk of having a permanent electronic recording made of our words (at p. 48, emphasis added).

[84] *Duarte*'s concern with the recording of private communications was rooted in the conviction that if members of the public believed that every time they spoke they were at risk of producing a documented record of their communications for the state to use at its sole discretion, privacy from state intrusion would no longer exist, and freedom of thought and expression would be effectively stripped of meaning: p. 44. Since 1990, it has therefore been accepted that to leave electronic state surveillance unchecked would be to relinquish our freedom: the "freedom not to be compelled to share our confidences with others is the very hallmark of a free society": p. 53.

[85] In response to *Duarte*, Parliament regulated participant electronic state surveillance: *R. v. Pires*, 2005 SCC 66, [2005] 3 S.C.R. 343, at para. 8. What is now

s. 184.2 of the *Code* provides that where the state seeks to "intercept" a "private communication", the state must obtain prior judicial authorization, even when one party to that communication has consented to its interception.

B. *Duarte for the Digital Age*

[86] This appeal "is *Duarte* for the digital age": A.F., at para. 69. In *Duarte*, state access to documentation of our private communications occurred via state recording technology. Now, however, individuals often communicate using electronic media, such that their conversations are inherently recorded. Where the intrusive technology used to be in the hands of the state, it is now in our back pockets.

[87] As La Forest J. clarified in *Wong*, the principles in *Duarte* must not be restricted to the particular technology at issue in that decision. Rather, *Duarte* was concerned with "all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future": *Wong*, at pp. 43-44. The electronic intrusion that lay at the heart of *Duarte* was the breach of the right to choose the range of our listeners, and the concomitant reality of having to contend with a documented record of our private thoughts in the hands of the state. *Duarte* framed this danger as the state recording and transmitting our words, but this privacy breach can present itself in many forms.

[88] In this case, we have the opportunity to pull the normative principles of *Duarte* and *Wong* through this Court's more recent *Charter* s. 8 and *Code* Part VI jurisprudence — in particular, *Patrick*; *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *Spencer*; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696; *Reeves*. The goal is to arrive at a judicial position that, while firmly grounded in the case law, "keep[s] pace with technological development, and, accordingly, . . . ensure[s] that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take": *Wong*, at p. 44.

[89] The risk contemplated in *Duarte* was that the state could acquire a compelled record of citizens' private thoughts with no judicial supervision. At the end of the Cold War era, the way to obtain a real-time *record* of a conversation was to *record* it. Today, the way to obtain a real-time record of a conversation is simply to engage in that conversation. This Court must assess how and whether the primary concern of documentation in *Duarte* still applies to cases in which (a) a communication method self-generates documentation of the communication, and (b) the originator of the communication *knows* that this occurs. Should this shift in communication technology now allow the state to access people's private online conversations at its sole discretion and thereby threaten our most cherished privacy principles?

[90] In my view, the answer is no. This Court must identify the privacy interest that *Duarte* and subsequent cases sought to protect and ensure that it remains protected as the communication environment evolves. This privacy interest is the right to be secure against surreptitious state access to records of our private thoughts with no judicial supervision. In order to safeguard this privacy interest, *Duarte* concluded that state access to electronic recordings of private communications requires regulation. A shift in communication methods should not mean that the state should no longer be required to seek authorization prior to surreptitiously acquiring written records of our private communications. If it were otherwise, "there would be no meaningful residuum to our right to live our lives free from surveillance": *Duarte*, at p. 44.

C. *It Is Objectively Reasonable to Expect That the State Will Not Acquire Records of Private Conversations at its Sole Discretion*

[91] Unregulated state access to electronic private communications engages s. 8 of the *Charter* because contemporary electronic communications are analogous to the surreptitious electronic recordings that attracted a reasonable expectation of privacy in *Duarte*. While electronic communications possess the characteristics of informality and immediacy that define oral conversations, they also possess the characteristics of permanence, evidentiary reliability, and transmissibility that define electronic recordings. They are a form of the "documented record" (*Duarte*, at p. 54, referring to *White*, at pp. 787-89) to which the state seeks access. Thus for the "freedom not to be compelled to share our confidences" (*Duarte*, at p. 53) to retain

any meaning, state access to electronic recordings of our private communications requires regulation. It was, therefore, objectively reasonable for Mr. Mills to expect not to be subjected to warrantless state acquisition of permanent electronic recordings of his private communications. The state action in this case constituted a search within the meaning of s. 8 of the *Charter*.

[92] In *Duarte*, La Forest J. distinguished between two different orders of state activity: "[A] conversation with an informer does not amount to a search and seizure within the meaning of the *Charter*. Surreptitious electronic interception and recording of a private communication does": p. 57; see also *R. v. Fliss*, 2002 SCC 16, [2002] 1 S.C.R. 535, at para. 12. In her reasons, my colleague Karakatsanis J. analogizes Mr. Mills' messages with "Leann" to *Duarte*'s "conversation with an informer": at paras. 42 and 48. In Karakatsanis J.'s view, the messages exchanged between Mr. Mills and Cst. Hobbs were analogous to an oral conversation, and s. 8 of the *Charter* was not engaged.

[93] With respect, I am of the view that when one grounds the distinction between a "conversation" and a "recording" within a discussion of the privacy interest that *Duarte* sought to protect, it becomes apparent that the electronic communications in the case at bar constituted *both* the conversation *and* the surreptitious electronic recording of that conversation. 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.

[94] This Court has already opined on the hybrid nature of text messaging. In *TELUS*, Abella J. stated that "text messaging bears several hallmarks of traditional voice communication: it is intended to be conversational, transmission is generally instantaneous, and there is an expectation of privacy in the communication": para. 1. Later in her judgment, Abella J. noted a distinction between text messaging and oral communication: "unlike voice communications, text communications, by their nature, generate a record of the communication which may easily be copied and stored": para. 34. Thus text messaging is "an electronic conversation": *TELUS*, at para. 5. While electronic communications can possess the immediacy and spontaneity of a "simple conversation", they also inherently generate a permanent[1] written record of the communication itself. In his concurring reasons in *Marakah*, Rowe J. reached a similar conclusion: digital communication both "creates a record that is beyond our control" and, at the same time, possesses a "conversational quality" that makes it "akin to a digital conversation": paras. 86-87. If *Duarte*'s dichotomy was concerned with documentation, this means that electronic communications occupy both sides of the ledger. They are both the oral conversation and the electronic recording of that conversation.

(1) The Significance of Creating the Recording Ourselves

[1] While all electronic communications generate a written record of a conversation, not all electronic communications generate a *permanent* written record, e.g. "Snapchat". Nonetheless, the general nature of electronic communication remains and must be addressed: "technical differences inherent in new technology should not determine the scope of protection afforded to private communications": *TELUS*, at para. 5.

[95] There is no doubt that, as Karakatsanis J. states, "Email and Facebook messenger users are not only aware that a permanent written record of their communication exists, they actually create the record themselves": para. 48. That conversants are aware that their communications are being recorded, and that they knowingly create the record themselves, does not mean that modern electronic communications must be analogized to the "oral conversation" in *Duarte* or destroy any reasonable expectation of privacy in those communications.

[96] In drawing a distinction between oral communication and recording, La Forest J. cited *Holmes v. Burr*, 486 F.2d 55 (1973), at p. 72: '"Few of us would ever speak freely if we knew that all our words were being captured by machines for later release before an unknown and potentially hostile audience. No one talks to a recorder as he talks to a person"': *Duarte*, at p. 50. Adapting *Duarte* to our digital age, it remains the case that no one speaks to a recorder as they would speak to a person. Yet people now "speak to recorders" each time they send an electronic message. Does this mean that it is no longer objectively reasonable to expect that our conversations will remain private, simply because they are now (much of the time) recorded? This Court has held in the negative. Creating written, electronic records of one's private communications is a virtual prerequisite to participation in society, and yet "Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives": *Jones*, at para. 45. Despite the capacity of modern technology to record electronic communications, individuals still retain both

subjective and objective expectations of privacy in those communications: *TELUS*, at para. 32; transcript, at p. 59.

[97] Further, 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. The standard is normative, not descriptive. As the Honourable Renee M. Pomerance wrote in "Flirting with Frankenstein: The Battle Between Privacy and Our Technological Monsters" (2016), 20 *Can. Crim. L. Rev*. 149, at p. 159:

> Citizens may be willing to give up civil liberties if they believe that it will make them safer. They may be resigned [to a lack of] privacy for the sake of convenience. They may be resigned to a lack of privacy, having been conditioned to believe that we are already living in a surveillance society. No one of those attitudes should singlehandedly shape our legal approach. Rights and freedoms should not be shaped by fear or fatalism.

[98] In *Duarte*, the danger inherent in the state's ability to create electronic recordings of our words at any moment and with no justification at all was that it would lead to a society in which we expected this to be the case. In La Forest J.'s view, a society in which we risk unregulated electronic surveillance "every time we ope[n] our mouths" (*Duarte*, at p. 44) is one that no longer has any sense of freedom: *Duarte*; *R. v. Wise*, [1992] 1 S.C.R. 527, at p. 565, per La Forest J. The intervener Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic discussed "the damage to free expression that would flow from imputing an assumption that one's interlocutor may be an undercover state agent making records of the electronic

conversation" (I.F., at p. 9) by referencing this passage by Alan Westin, who was writing about the early development of computers (*Privacy and Freedom* (1967), at p. 349):

> The danger to privacy and to . . . liberties in this development was that individuals who knew that all this information was being collected and stored and lay readily available in machines would never be able to know when it would be used "against them" and for what purposes. This public awareness of potential use would lead to an "increase in behaviour 'for the record'" and less freedom of action and expression. People will be concerned not only with the fact that they are going "on record," but also with how that record will "look" to those in authority who examine it. The whole purpose of privacy . . . is to allow for unguarded, experimental "release" behavior of individuals, and this outlet is just what our dossier-computer system is threatening.

Harlan J. expressed this same sentiment as follows: "[a]uthority is hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed": *White*, at pp. 787-89, referenced in *Duarte*, at p. 54.

[99] Fifty years on from *White*, authority is beginning to emerge, and it is corroborating Harlan J.'s views. A number of empirical studies have confirmed the "chilling effect" of government surveillance on online behaviour. These studies suggest that state electronic surveillance leads individuals to self-censor their online expression: J. W. Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017), 6:2 *Internet Policy Review* 22 (online); A. Marthews and C. Tucker, "The Impact of Online Surveillance on Behavior" in

D. Gray and S. E. Henderson, eds., *The Cambridge Handbook of Surveillance Law* (2017) 437.

[100] The consequences of knowing that, at any point and with reference to any of our statements, we will have to contend with a documented record of those statements in the possession of the state, would be no less than the total "annihilat[ion]" (*Duarte*, at p. 44) of our sense of privacy. For this reason, *Duarte* decided that if the state wished to acquire documentation of the private thoughts of its citizens, it would require prior judicial authorization.

(2) "Intended Recipient"

[101] Karakatsanis J. states that "it is not reasonable to expect that your messages will be kept private from the intended recipient": at para. 36. That general proposition does not and cannot apply when the state has secretly set itself up as the intended recipient. It is clear from *Duarte* that in the case of state participant surveillance, the notion of "intended recipient" — as well as the characterization of "the person or persons to whom we direct our remarks" (Karakatsanis J.'s reasons, at para. 50, citing *Duarte*, p. 47) — is infused with the concept of the right to choose the range of one's listeners. While in *Duarte* the "intended recipients" of the conversation were the undercover police officer and the informer, Mr. Duarte retained a reasonable expectation of privacy in the contents of that conversation because the police use of recording technology violated his right not to have to contend with a documented record in the hands of the state. Analogously, an individual engaged in a private,

electronic conversation retains the reasonable expectation that the state will only have access to a permanent electronic recording of that private communication if the state agent has sought judicial authorization. Normative expectations have not changed. The difference, of course, is that we now use technology that makes the recording itself.

[102] I note that this appeal concerns electronic communications and their conscriptive capacity to inherently generate a record of what will often be spontaneous, informal communication. It does not concern the privacy interests in a note, a letter, or other written forms of communication that will turn on their own qualities: Karakatsanis J.'s reasons, at para. 45; *Marakah*, at para. 86, per Rowe J.; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at para. 24.

(3) Quantitative and Qualitative Distinctions Between In-Person and Electronic State Surveillance

[103] Two additional comments on the nature of electronic surveillance are in order. First, the "conversations" contemplated by this Court in *Duarte* do not afford a direct comparison to electronic communications today because the in-person conversations with undercover police officers at issue in *Duarte* were not capable of subjecting the public to surreptitious electronic surveillance on a mass scale.

[104] In a free and democratic society, individuals do not expect a significant number of the people with whom they interact to be undercover police officers

surveilling them at the officers' "whim": *Duarte*, at pp. 44 and 49. While such a scenario is inconceivable in in-person undercover operations due to the practical resource constraints of undercover police work, it is perfectly conceivable when it comes to electronic surveillance technologies: "surveillance has emerged as the dominant organizing practice of late modernity, and is used in different technological guises to monitor and govern assorted categories of people (citizens, motorists, workers, students, consumers, international travelers, military adversaries, welfare recipients, and various other groupings)": K. D. Haggerty, "Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance" (2009), 17 *Critical Crim*. 277, at pp. 277-78; see also D. Lyon, *Surveillance After Snowden* (2015), at p. 47: "the cables and conduits of the internet . . . make possible mass surveillance as never before".

[105] In part, this is a question of resources. While an in-person undercover operation will usually occur at a 1:1 ratio (one police officer gaining the confidence of one target), online surveillance may cover much more ground. A single police officer can conduct many electronic conversations at once. Thus the number of electronic conversations that undercover police officers could be conducting with members of the public at any given time is likely to be greater than the number of conversations that the same police officers could conduct in person.

[106] The analogy between an oral conversation and an electronic communication is not only untenable because of the quantitative increase in

surveillance capacity when it moves online; there is also a qualitative distinction between electronic surreptitious surveillance and in-person surveillance. Cst. Hobbs could not have been conducting this police work in person. The ability to fabricate alternative identities has never been more possible than it is now. Of course, this aspect of electronic communication makes it all the more necessary to police online spaces for criminal activity that thrives on such anonymity. Yet this same anonymity allows for a different order of state surveillance in which police officers can more easily create a richly textured, and therefore more believable, false identity through which to conduct surveillance. Left to conduct electronic surveillance at their sole discretion — because "when undercover police officers communicate in writing with individuals, there is no 'search or seizure'" (Karakatsanis J.' reasons, at para. 36) — the police "could impersonate an internet therapy provider to learn of a person's addictions or an online dating service to discover an individual's sexual preferences — all for weeks or months on end": I.F., Criminal Lawyers' Association, at para. 4. Where, as here, the police can pose as a child and gain the trust of other children — or where, for instance, the police can impersonate an internet therapy provider or online dating service through intricately fabricated false identities — the nature of surveillance has changed. Our privacy protections must keep pace.

[107] In her reasons, Karakatsanis J. states that "rogue police undercover investigations" should be appropriately characterized as a threat to the integrity of the justice system itself: para. 62. She looks to mechanisms such as abuse of process and the entrapment doctrine to redress these types of police tactics: paras. 62-63. I agree

that police action that "offends our basic values" (*Rothman v. The Queen*, [1981] 1 S.C.R. 640, at p. 689, per Lamer J.) can and should be addressed in a number of ways; this is for the good. However, when that state action also intrudes on a reasonable expectation of privacy, it is intended to be addressed, *inter alia*, via s. 8 of the *Charter*. What is at issue in this appeal is not only the actions of one officer, but also the general rule that should govern how the state may gain access to private communications using current technologies. In my view, placing communications outside s. 8 because the state recipient can now obtain a record of the conversation simply by engaging in it, undermines the purpose of privacy rights and upsets the careful balance between the ability of the state to investigate crime and the rights of individuals to private areas of expression.

[108] *Duarte* was concerned about the privacy implications of the *state* acquiring permanent, electronic recordings of private communications at its sole discretion. Electronic communications are conversations that occur on platforms that inherently have the capacity to generate permanent electronic recordings. If the state wishes to acquire the documentation of those communications, it requires authorization.

D. *The Question of Relationship*

[109] My colleague Brown J. decides this appeal on the basis that there is no reasonable expectation of privacy where the state conducts a sting operation and knows from the outset that an adult accused is communicating with a child that he or

she does not know: paras. 22-3. While Brown J. ties his conclusion to the sting context, his reasoning would apply whenever its "crucial" factors are present: that the accused "was communicating with someone he believed to be a child, who was a stranger to him": para. 22 (emphasis deleted).

[110] With respect, I do not accept that this new category of "relationship" is needed to limit when there is a reasonable expectation of privacy. 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. Over and above these conflicts with s. 8 jurisprudence, at the heart of this reasoning is the normative position that a relationship between an adult and a child who is a stranger is not a relationship worthy of s. 8's protection: Brown J.'s reasons, at para. 26. This position seeks to put 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, and which do not. The concern here is not only that this has never been done before — it is that, as a matter of principle in the s. 8 context, it should not be done at all. Judicial (dis)approbation of an accused's lifestyle has no place in the s. 8 privacy analysis.

[111] The Court should not create *Charter*-free zones in certain people's private, electronic communications on the basis that they might be criminals whose

relationships are not socially valuable. The *Charter* expressly grants s. 8 protections to "everyone". Members of society have a reasonable expectation that their private, electronic communications will not be acquired by the state at its sole discretion.

[112] Finally, a finding of reasonable expectation of privacy in a particular thing or area does not mean that the state is forbidden from conducting a search — it simply means that the police action must be supported by a power or authorization that respects s. 8 of the *Charter*. In my view, the scenario presented of a sting context in which the state pretends to be a child and communicates with those seeking to sexualize children is precisely the type of circumstance in which the state could and should obtain judicial authorization to surveil private, electronic communications.

(1) Relationship as a Proxy for Control

[113] My colleague Brown J. states that it is not reasonable for an adult to expect privacy when communicating with a vulnerable child who is a stranger because hoping that a complete stranger will keep one's communications private is a "gamble" that cannot ground an objectively reasonable expectation of privacy: see Brown J.'s reasons, at paras. 22-23. In other words, Mr. Mills did not have a reasonable expectation of privacy from warrantless, surreptitious state electronic surveillance because he did not have sufficient *control* over what his co-conversant would do with his communications.

[114] With respect, this position reintroduces the "loss of control due to risk of disclosure" analysis that this Court recently rejected in *Marakah*. A reasonable expectation of privacy analysis concerns state intrusion. The risk that one's co-conversant may disclose a private communication does not affect the reasonableness of the expectation that the state, in the absence of such disclosure, will not intrude upon that private communication. For this reason, the theory of loss of control due to risk of disclosure is a type of risk analysis that this Court has repeatedly said should not form part of the s. 8 analysis: *Duarte*, at p. 44; *Wong*, at pp. 45-46; *Wise*, at pp. 563-64, per La Forest J., dissenting but not on this point; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34, per Deschamps J., concurring; *Cole*, at para. 58; *Marakah*, at para. 45; *Reeves*, at para. 50; see also *Ward*, at para. 77; *R. v. Craig*, 2016 BCCA 154, 335 C.C.C. (3d) 28, at para. 108.

[115] This Court's rejection of risk analysis has never hinged on the nature of the relationship between the parties. In *Marakah*, for instance, the majority did not analyze the relationship between Mr. Winchester and Mr. Marakah. This is because it was not relevant to the question of whether Mr. Marakah had a reasonable expectation that the *state* would not access his text messages from a recipient's device without a warrant. Thus *Marakah*'s rejection of risk analysis, at para. 40, was a statement of general principle applicable to all reasonable expectation of privacy assessments of electronic communications, including the assessment to be undertaken in the case at bar:

> The Crown argues that Mr. Marakah lost all control over the electronic conversation with Mr. Winchester because Mr. Winchester *could* have disclosed it to third parties. However, the risk that recipients can disclose the text messages they receive does not change the analysis: *Duarte*, at pp. 44 and 51; *Cole*, at para. 58. To accept the risk that a co-conversationalist could disclose an electronic conversation is not to accept the risk of a different order that the state will intrude upon an electronic conversation absent such disclosure. "[T]he regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words": *Duarte*, at p. 44. Therefore, the risk that a recipient could disclose an electronic conversation does not negate a reasonable expectation of privacy in an electronic conversation. [Underlining added.]

[116] The focus of a reasonable expectation of privacy analysis is not on whether the party to whom one has communicated is likely to go to the police — "[n]o set of laws could immunize us from that risk": *Duarte*, at p. 44. Rather, the focus is on whether, absent such disclosure, it is reasonable to expect that the police will not intrude on those communications without a warrant or some other form of authorization.

(2) Relationship as a Means of Targeting Illegality

[117] My colleague Brown J. concludes that because this Court has pronounced on the vulnerability of children, the capacity of the internet to facilitate sexual crimes against children, and the need to protect children from sexual exploitation, it follows that "adults cannot reasonably expect privacy online with children they do not know": para. 23. With the greatest of respect, I cannot read this conclusion as anything other than the targeting of illegal activity and the denial of privacy rights to individuals

who, it may be believed, are most likely to engage in that type of illegal activity. The centrality of the sting context in my colleague's analysis only highlights this further: a sting operation — by definition — targets illegal activity. As such, the conclusion that "adults cannot reasonably expect privacy online with children they do not know" is contrary to the core principle of content neutrality at the heart of this Court's s. 8 jurisprudence.

[118] Under s. 8, the fact that an individual may be engaged in criminal behaviour online does not affect the reasonable expectation of privacy analysis. This Court has consistently said that "[t]he nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought": *Spencer*, at para. 36; *Hunter*, at p. 160; *Wong*, at pp. 49-50; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569, at para. 72; *Patrick*, at para. 32; *Marakah*, at para. 48. For this reason, a reasonable expectation of privacy analysis must be framed in "broad and neutral terms": *Wong*, at p. 50.

[119] Before this Court, the Crown acknowledges that the majority in *Marakah* held that a reasonable expectation of privacy analysis must be content neutral. However, the Crown urges this Court to depart from its content neutral approach in all cases of electronic communications "that constitute a crime against the recipient": R.F., at para. 56.

[120] By stating that "adults cannot reasonably expect privacy online with children they do not know," Brown J. is effectively granting the Crown's request to find a "limited exception" (R.F., at para. 50) to this Court's content neutral analysis. With respect, there is no reason to depart from well-established principle and recent precedent in this case. This is not the first time that the Court has been called upon to develop privacy law in the context of digital and/or internet-based sexual crimes involving minors: see e.g. *Cole*, *Spencer*, and *Reeves*. This Court did not see fit to displace its content neutral analysis in those cases, and it is no more appropriate to do so here.

[121] The standard reasoning underpinning the importance of a content neutral analysis is that justifying a search based on the illegal content discovered during that search undermines the system of prior judicial authorization meant to prevent unjustified searches before they occur: see *Hunter*, at p. 160. Brown J. seeks to allay that concern by targeting only those individuals who, according to my colleague, deserve to be searched because their relationships are not ones that our society would wish to shield from state scrutiny — in this case, adults who communicate online with children they do not know.

[122] This approach assumes that communications between adults and children who do not know each other will be criminal in nature. In reality, this is not an inevitability. The broad category of "relationships between adults and children who are unknown to them" encompasses informal, vitally-important educational

relationships that can arise in online spaces. This wide net is therefore overbroad and would capture an array of non-criminal communications: for example, professionals who communicate with youth to provide career advice, or adults who may be able to offer support to youth struggling with addiction, sexual identity or bullying because they have had similar life experiences. An adult sharing their own experiences, in the course of a private, electronic communication between strangers could make all the difference in a young person's life. If there is no reasonable expectation of privacy in such communications because an adult is in contact with an unknown child, then the state is permitted to listen in and record without the need for any regulation, authorization or limits. Content neutrality was developed to ensure that such unjustified state intrusions into privacy would not occur.

[123] In my view, and following Binnie J. in *A.M.*, the position that "adults cannot reasonably expect privacy online with children they do not know" shifts the analysis from a "reasonable" expectation of privacy to a "legitimate" expectation of privacy. The view that some relationships are *a priori* criminal and therefore do not *legitimately* attract an expectation of privacy both assumes criminality where there may be none, and assumes that there can be no reasonable privacy interests in illegal communications. Both of these assumptions are incorrect: *A.M.*, at paras. 69-73.

[124] Finally, as I discuss in further detail later in these reasons, the police in the case at bar engaged in unregulated online surveillance of an unknown number of youth who believed they were speaking to someone their own age. The facts of this

case, therefore, do not illustrate the scenario that my colleague envisions — a scenario in which only criminals are denied privacy protection.

[125] Remember that the issue is not whether a child who has been victimized can go to the police with an online communication received by that child. Rather, the issue is whether the state can pretend to be a child in private online communications at its sole discretion and absent any regulation. In my view, it should not be free to do so.

(3) Courts Should Not Be in the Business of Determining Which Personal Relationships Fall Within Section 8

[126] Beyond my concerns about content neutrality, I would also caution that the normative position that "adults cannot reasonably expect privacy online with children they do not know" asks courts to engage in an unnecessary and unprincipled valuation of personal relationships when this factor is irrelevant to the s. 8 inquiry. Further, even if assessing personal relationships to determine which of them deserve to be protected from warrantless state scrutiny did accord with the s. 8 inquiry, courts are ill-equipped to conduct this assessment. Casting suspicion on an entire category of human relationship not only stigmatizes that relationship — it exposes meaningful and socially valuable communication to unregulated state electronic surveillance. For all of these reasons, in my view, courts should not use s. 8 to allow the state into certain personal relationships which are seen as unworthy of *Charter* protection.

[127] I say this understanding that as the majority of this Court stated in *Patrick*, "[p]rivacy analysis is laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy": para. 14. Yet the necessity of conducting "value judgments" does not permit courts to engage in a free-wheeling evaluation of accused persons and their relationships. Rather, the *Charter* has tasked courts with making value judgments *that relate to the objects of the s. 8 inquiry itself*. These objects are "the privacy of the area or thing being searched and the potential impact of the search on the person being searched": *Patrick*, at para. 32. On this basis, this Court has assessed whether members of society can expect privacy in their backpacks in school (*A.M*); in their text message communications, be that in a search incident to arrest (*R. v. Fearon*, 2014 SCC 77, [2014] 3 S.C.R. 621) or on a recipient's device (*Marakah*); in computers in their own home (*Vu*; *Reeves*); in a car that they do not own (*R. v. Belnavis*, [1997] 3 S.C.R. 341); and in the relative distribution of heat over the surface of their home (*Tessling*).

[128] The s. 8 inquiry is not, and never has been, focused on whether a relationship between two non-state actors is worthy of constitutional protection. For example, *R. v. Dyment*, [1988] 2 S.C.R. 417, did not concern relationships. The privacy invasion in *Dyment* was "the use of a person's body without his consent to obtain information about him": pp. 431-32.

[129] Nor is the value of a personal relationship an appropriate object or aspect of a s. 8 inquiry. Parliament has expressly extended s. 8 protection to "everyone": "Everyone has the right to be secure against unreasonable search or seizure." Respectfully, it is not the role of the courts to evaluate personal relationships with a view to denying s. 8 *Charter* protection to certain classes of people. Rather, as stewards of the *Charter*, courts "provide what is often the only effective shelter for individuals and unpopular minorities from the shifting winds of public passion"': *R. v. Collins*, [1987] 1 S.C.R. 265, at p. 282, citing D. Gibson, *The Law of the Charter: General Principles* (1986), at p. 246.

[130] Moreover, carving out privacy-free zones for particular relationships will expose socially meaningful communications to unregulated state surveillance. As detailed above, there are many communications that would be captured in the category of "adults who communicate with children who are unknown to them" that are worthy of s. 8's protection.

[131] For all of these reasons, a new turn in our s. 8 jurisprudence that looks to the personal relationships between parties as a dispositive means of denying or granting privacy rights conflicts with the purpose of s. 8. It effectively sanctions the unjustified state intrusion into swaths of all individuals' private lives in the hopes of capturing some illegal communications. This runs counter to this country's decision that private communications are to remain private, unless the state has authorization to search them.

(4) Conclusion on the Question of Relationship

[132] This Court has consistently rejected the risk analysis approach, and instead conducts content neutral s. 8 analyses by examining the state conduct at issue. The question to be answered when conducting a reasonable expectation of privacy analysis in the case at bar is not whether adults who communicate online with underage strangers during alias-based sting operations have a reasonable expectation of privacy in their private, electronic communications. Rather, it is whether members of society have a reasonable expectation that their private, electronic communications will not be acquired by the state at its sole discretion: see *Patrick*, at para. 32.

E. *Conclusion on Reasonable Expectation of Privacy*

[133] In a free and democratic society, it is reasonable for members of society to expect that the state will only access electronic recordings of their private communications if it has sought authorization to do so. This includes participant surveillance of one's private communications. It may be difficult for some to accept that this reasonable expectation of privacy extends to Mr. Mills as well, but extend it does: "[t]he question is not which risks the claimant has taken, but which risks should be imposed on him in a free and democratic society": *Reeves*, at para. 41; *Duarte*, at p. 52; *Spencer*, at para. 36; *Patrick*, at para. 32; *Wise*, at p. 567. The police surveillance in question constituted a search within the meaning of s. 8 of the *Charter*.

V. Part VI Authorization

[134] I agree with the appellant that "the use of 'Snagit' to capture the messages fits within the definition of 'intercept' in s. 183 of the *Code* as this program recorded and acquired the substance of the texts": A.F., at para. 48; see also Decision Re s. 8, at para. 34. I further explore whether Cst. Hobbs' actions may also have constituted an interception even in the absence of "Snagit". This latter discussion raises the issue of whether our statutory scheme authorizing the interception of private communications requires reconsideration in light of shifts in communication technology. I leave this reconsideration to Parliament's good judgment.

A. *Did Mr. Mills Have a Reasonable Expectation of Privacy in His Communications?*

[135] For s. 184.2 to apply to a particular investigative technique, the state must be seeking to intercept a "private communication". A "private communication" is "any oral communication, or any telecommunication . . . that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it": *Code*, s. 183. Built into this definition is the requirement that the originator had a reasonable expectation of privacy in their communication. For the reasons outlined above, Mr. Mills had a reasonable expectation of privacy in his communications. The impugned communications therefore constitute "private communication" under s. 183 of the *Code*.

B. *Did the Use of "Snagit" Constitute an Interception?*

[136] Section 184.2 of the *Code* applies to communications that have been "intercepted" by means of any electro-magnetic, acoustic, mechanical or other device. To "intercept" means to "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof": *Code*, s. 183. With respect for the opposing view, I conclude that the use of "Snagit" in this case constituted an interception.

[137] Cst. Hobbs recorded the conversations that he had with Mr. Mills using a computer program "which allows the computer user to capture and copy the information on the screen": Decision Re s. 8, at para. 6. When asked why he used this computer program, Cst. Hobbs replied, "[f]or continuity purposes to keep them all together for the sake of reproduction for the courts if need be": A.R., vol. II, at p. 7. He stated that he did not at any point print the messages directly from their original programs, but rather "would always save them by doing a screen capture": p. 8. Cst. Hobbs further explained: "every person may have their own way of doing things. That's just my personal preference which I found has always been more beneficial. I just find it keeps everything in the same location. I can store it all on my computer in the same file folder": p. 8. On the plain meaning of "record", Cst. Hobbs recorded the informational content of the private communications when he "save[d] them by doing a screen capture" into a centralized location on his computer "for the sake of reproduction for the courts" (pp. 7-8). This constituted an interception: see also ***R. v. Kwok***, [2008] O.J. No. 2414 (QL)(C.J.).

[138] The interception in this case occurred in "real-time": *Jones*, at para. 69. This Court's analysis of the meaning of "intercept" in *Jones* clarified that an "interception suggests a prospective concept of authorization relating to communications not yet in existence. The word 'intercept' denotes an interference between the sender and recipient in the course of the communication process": *Jones*, at para. 69; see also *TELUS*, at para. 37. Thus Part VI is a regulatory scheme intended to authorize the real-time interception of future communications. I agree with the appellant that, for this reason as well, Part VI applies to the state action here: A.F., at para. 59. Cst. Hobbs received the communications and contemporaneously recorded them using screen capture software. This was far from the historical text messages at issue in *Jones*. Had Cst. Hobbs sought authorization to conduct these real-time interceptions, he would have been seeking authorization to intercept communications that were not yet in existence. The state action in this case thus conforms to this Court's interpretation of "interception" in *Jones*.

[139] I further note that, contrary to what the Court of Appeal held (at para. 13) and what some other appellate courts and commentators appear to have decided as well (2017 NCLA 12; see also *R. c. Blais*, 2017 QCCA 1774, at paras. 16-17 (CanLII), *R. v. Beairsto*, 2018 ABCA 118, 349 C.C.C. (3d) 376, at para. 25), an "interception" does not require a third party. This Court's reference to third-party involvement in *Jones* (at para. 72) does not apply to cases of participant surveillance or to the parameters of s. 184.2 of the *Code*. Parliament enacted what is now s. 184.2 in response to *Duarte*. *Duarte* was a case of participant surveillance — the

undercover officer and informer in that case were *participants* in the conversation. The "interception" in *Duarte* occurred not because a third party intercepted the communication, but because state recording equipment did. The trial judge correctly conducted this analysis: Decision Re s. 8, at paras. 17 and 23.

[140] Finally, concluding that the state action in this case was an "interception" accords with the "undergirding purpose" of Part VI: *Jones*, at para. 59; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27, at para. 21. Part VI is aimed at the use of intrusive technologies to surveil private communications: *Jones*, at para. 73; *Duarte*, at pp. 43-44. In employing screen capture software, Cst. Hobbs used technology to surveil — record and acquire in real time — Mr. Mills' private communication and, in so doing, violated Mr. Mills' right to choose the range of his listeners: *Duarte*, at p. 51.

C. *Surreptitious Electronic Communication by the State With Members of the Public in a Private Setting May Constitute an Interception*

[141] In our current communications environment, we are wiretapping ourselves. We knowingly deliver documentary evidence of our private communications into the hands of not only our intended recipients, but also into the digital repositories of corporate third parties. Yet this does not negate the right to be protected against *state* intrusion on our privacy. As the statutory scheme with which we regulate state privacy intrusion, Part VI must engage with and accommodate these complexities. This includes the constituent components of Part VI, such as the

definition of "intercept": "The issue then is how to define 'intercept' in Part VI. The interpretation should be informed not only by the purposes of Part VI, but also by the rights enshrined in s. 8 of the *Charter*, which in turn must remain aligned with technological developments": *TELUS*, at para. 33.

[142] The statutory definition of "intercept" is to "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof." In communicating with Mr. Mills over a medium that inherently produces an electronic recording,[2] Cst. Hobbs "acquired" a record of the communication. It is true that, leaving the issue of "Snagit" aside, Cst. Hobbs simply availed himself of the technology that Mr. Mills was already using. Yet just as *Duarte* was not aimed solely at the *recording* of the conversation but also at the state's acquisition of a *record*, s. 184.2 is not only aimed at intrusive technologies that *interfere* in private communications (*Jones*, at para. 69); it is also aimed at the capacity of intrusive technologies to *access* our private communications: "Part VI recognizes the dangers inherent in permitting access to the future private communications of a potentially unlimited number of people over a lengthy period of time": *TELUS*, at para. 42. Members of the public must be protected from unregulated, surreptitious state collection of their private electronic communications. It may therefore be the case

[2] It must be noted, however, that in this case the inherent documentary evidence produced by virtue of communicating over Facebook and Hotmail was not the evidence adduced at trial. Cst. Hobbs' only copy of the messages were those that he had acquired via "Snagit". He had deactivated "Leann's" Facebook account when Mr. Mills was charged with the offences now before this Court. As for the record of conversations on Mr. Mills' end, the search of Mr. Mills' hard drive pulled up only fragments of the communications, the evidentiary weight of which depended on checking the fragments against the integral copy captured by "Snagit". The only reproducible form of the communications came from the screen captures.

that the surveillance of Mr. Mills' online private communication, with or without screen capture technology, constituted the type of clandestine state surveillance using intrusive technology that Part VI was intended to proscribe.

[143] If, in the alternative, surreptitious, electronic police surveillance of private communications is only regulated by Part VI to the extent that extraneous recording software is employed, then our "comprehensive scheme…for the interception of private communications" (*TELUS*, at para. 2) is no longer sufficiently comprehensive. To be constitutionally compliant, state acquisition in real-time of private electronic communications requires regulation.

D. *Part VI Strikes the Right Balance Between Law Enforcement's Need to Investigate Crime and the Right of an Individual in a Democratic Society to be Left Alone*

[144] I agree with the intervenor the Attorney General of Ontario that the internet has created "an unprecedented platform for child exploitation" and that undercover proactive police investigations are necessary to combat the online exploitation of children: I.F., at pp. 7-9; see also G. J. Fitch, Q.C., "Child Luring" in *Substantive Criminal Law, Advocacy and the Administration of Justice*, vol. 1, presented to the National Criminal Law Program (2007), at pp. 1 and 3. Part VI of the *Code* was developed with these considerations in mind. In my view, its application to the use of "Snagit" in the case at bar strikes the right balance between law enforcement's need to investigate crime and the right of an individual in a democratic society to be left alone. Where the police wish to conduct surreptitious electronic

surveillance by means of intrusive technology, their investigative methods must be authorized by the judiciary or some other independent third party.

[145] I am not persuaded by the argument that internet predators move so quickly from victim to victim that it would be "unconscionable" to pause an investigation for the amount of time that it would take to secure judicial authorization (I.F., Canadian Association of Chiefs of Police, at pp. 6-8). Our judicial system is equipped to issue authorizations in a timely fashion. Police officers secure warrants on short timelines every day in this country. Here, the words of La Forest J. in *Duarte*, at pp. 52-53, are apt:

> . . . the imposition of a warrant requirement would have the sole effect of ensuring that police restrict "participant monitoring" to cases where they can show probable cause for a warrant. It is unclear to me how compelling the police to restrict this practice to instances where they have convinced a detached judicial officer of its necessity would hamper the police's ability effectively to combat crime. But even if this were so, this restriction would be justified by the knowledge that the police would no longer have the right 'to train these powerful eavesdropping devices on you, me, and other law-abiding citizens as well as the criminal element', to cite the observation of Cirillo J. in *Commonwealth v. Schaeffer*, [536 A.2d 354 (Penn. 1987)], at p. 367.

Or, as Karakatsanis J. succinctly states in *Reeves*, at para. 54: "I recognize that rejecting the Crown's approach may interfere with criminal investigations. But *Charter* rights often do."

[146] I acknowledge, however, that the implications of concluding that the police "intercepted" the communication even absent the use of "Snagit" are more

complex. The question as to what standard of reasonableness would be required for prior judicial authorization of varied forms of proactive police investigations is one best left to Parliament. On this point, I take care to restate that my position does not and should not inexorably lead to the police being unable to investigate child lurers. Rather, it focuses on the *authorization* of those investigations by an independent third party. A less exacting regime than Part VI may be appropriate in certain circumstances.

[147] Finally, on the subject of "proactive police investigations" such as occurred in the case at bar, I would suggest that these investigations would benefit from a standardized set of privacy protective guidelines. According to Cst. Hobbs, there were no guidelines or policies available to assist him in setting up a minimally intrusive false identity. As a result, he created policy on his own, with undesirable consequences. To construct his online persona, Cst. Hobbs used photographs from the internet of a youth who was unknown to him. That youth was, therefore, unwittingly conscripted into a police investigation. Further, "[t]here were a number of what has been described by various authors as 'low visibility' encounters with [Cst. Hobbs] by innocent members of the public. The officer used their [online] presence on his Facebook page to provide credibility to his profile while at the same time they shared information with him unaware that he was a police officer": (2014), 346 Nfld. & P.E.I.R. 102, at para. 10 ("Decision re Section 24(2)"). Cst. Hobbs did not seek or obtain the informed consent of the individuals that he added on Facebook, individuals who were effectively used "as part of the 'bait' to trap an Internet predator": (2015),

364 Nfld. & P.E.I.R. 237, at para. 18 ("Sentencing Decision"). There was also no evidence as to how or whether the police retained the personal information of any of these individuals: Sentencing Decision, at para. 18. Proactive online 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. To ensure that such investigative techniques are minimally invasive, they must be subject to clear guidelines.

VI. Did the Search Breach Section 8 of the *Charter*?

[148] A search or seizure is presumptively unreasonable in the absence of prior judicial authorization. However, the Crown may establish, on a balance of probabilities, that the police conduct was reasonable in that it was authorized by law, the law was reasonable, and the manner in which the search was carried out was reasonable: *Collins*, at p. 278. Here, there was no prior judicial authorization and as such, the search is presumptively unreasonable. The search or seizure was not authorized by any law. Therefore, the search of the communications breached s. 8 of the *Charter*.

VII. Should the Evidence be Excluded Under Section 24(2) of the *Charter*?

[149] Having found that Mr. Mills' s. 8 *Charter* rights were breached, the trial judge nevertheless denied Mr. Mills' application to exclude the evidence of the electronic communications pursuant to s. 24(2). Though my reasoning differs in

several important respects, I agree with the trial judge that the admission of the evidence would not bring the administration of justice into disrepute.

[150] Mr. Mills argues that the trial judge ought to have approached this matter from the viewpoint that this was a violation of the right against self-incrimination. If this was Mr. Mills' position at the time that the application to exclude was heard, then I agree that the trial judge should have addressed it. However, even if this was an error, it had no effect on the outcome of the decision. In his sentencing decision, the judge found that this was not a case of entrapment: paras. 3-8. Thus, if he had canvassed this issue in his s. 24(2) analysis, the trial judge would have concluded that the evidence was not obtained contrary to the right against self-incrimination.

[151] The remainder of Mr. Mills' submissions concern the treatment and weighing of the factors for exclusion of evidence under s. 24(2) as articulated in *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353, at para. 71. These factors are: "(1) the seriousness of the *Charter*-infringing state conduct . . . (2) the impact of the breach on the *Charter*-protected interests of the accused . . . and (3) society's interest in the adjudication of the case on its merits".

[152] Mr. Mills submits that the trial judge erred in finding that the undercover officer acted in good faith. However, this was a reasonable conclusion open to the trial judge, who found that the police officer was "following what he believed to be a legitimate investigative technique": Decision re Section 24(2), at para. 10. It is concerning that the officer did not enquire into whether the investigative technique

was constitutionally valid, or into whether he was required to obtain judicial authorization: "negligence or wilful blindness cannot be equated with good faith": *Grant*, at para. 75. It is also concerning that there were no written police guidelines for him to follow. Yet in my view, Cst. Hobbs would be forgiven for assuming the constitutional validity of this technique. This Court's decision in *R. v. Levigne*, 2010 SCC 25, [2010] 2 S.C.R. 3, can be interpreted as validating the investigative technique used here[3]. The parties in *Levigne* did not raise the s. 8 *Charter* issues inherent in the police investigative tactics employed in that case, and thus this Court's silence on the issue in *Levigne* does not bind it now. Nevertheless, for this reason and for the reasons identified by the trial judge, the trial judge did not err in finding that the officer was acting in good faith. This first factor weighs in favour of admission.

[153] With respect to the impact on the accused's *Charter*-protected interests, the trial judge found that there was a reduced expectation of privacy because "The accused had been communicating with an unknown individual with the knowledge that his communications would be recorded on that person's computer": Decision re Section 24(2), at para. 11. As such, the trial judge found that this branch of the inquiry favoured admission of the evidence. Mr. Mills submits that the trial judge's findings run counter to the jurisprudence. I agree. There was no "reduced expectation of privacy" in this case. This Court has made clear that a person's lack of control over their communications does not reduce their reasonable expectation of privacy from

[3] In *Levigne*, the investigating officer employed a recording software program called Camtasia to record his private online chats with the accused. As the officer in that case testified, Camtasia is "a software program that basically records whatever happens on your screen as a video": *Levigne*, Appellant Record, at p. 113.

state intrusion: see *Duarte*, at p. 48; *Marakah*, at para. 68. The *Charter* breach substantially impacted Mr. Mills. It revealed private information that was central to his biographical core, and it exposed that information to police scrutiny: *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293 (a biographical core of information "would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual"); *Cole*, at paras. 45-46. This factor weighs in favour of exclusion.

[154] As for society's interest in the adjudication of the case on its merits, the trial judge found that the exclusion of the evidence would be "fatal to the Crown case", and that the evidence was "real probative evidence of high reliability": Decision re Section 24(2), at para. 12. On appeal to this Court, the appellant acknowledges that the offence in this case is serious. However, Defence counsel urges this Court not to place "undue emphasis" on the seriousness of the offence: A.F., at paras. 103-6.

[155] In my view, the balance of the three factors favours admission of the evidence. In so concluding, I do not place "undue emphasis" on the seriousness of the offence. While the impact of the breach on Mr. Mills' privacy interest was significant and not diminished, the seriousness of the *Charter* breach was minimal. I am of the view that the exclusion of "relevant and reliable evidence" in a child-luring case, obtained using tactics that the police had good reason to believe were legal at the time of the investigation, would bring the administration of justice into disrepute: *Grant*, at para. 81.

[156] The trial judge did not err by declining to exclude the evidence pursuant to s. 24(2), and I would uphold his determination that the appropriate remedy for the *Charter* breach is a two-month reduction in sentence.

VIII. Conclusion

[157] It was objectively reasonable for Mr. Mills to expect that a permanent electronic recording of his private communications would not be surreptitiously acquired by an agent of the state absent prior judicial authorization. Cst. Hobbs' use of "Snagit" constituted an "interception" within the meaning of Part VI of the *Code*. Further, even in the absence of "Snagit", it may be that the state investigative technique employed here constituted an "interception". Because Cst. Hobbs did not seek and obtain prior judicial authorization pursuant to s. 184.2 prior to using "Snagit", the search of the private communications was unreasonable. However, I would not exclude the communications under s. 24(2) of the *Charter*.

[158] This appeal raises serious questions as to whether and how police surveillance of electronic communications should be regulated. Following this Court's rich line of case law developing the normative principles of what constitutes a reasonable expectation of privacy, I conclude that unchecked state surveillance — in this case, unchecked state acquisition of permanent electronic recordings of private communications — contravenes s. 8 of the *Charter*. To the extent that our legislative scheme authorizing the interception of private communications does not capture the

modern methods by which the state obtains real-time recordings of private communications, I believe that it requires reconsideration.

[159] For the foregoing reasons, I would dismiss the appeal.

Appeal dismissed.

Solicitors for the appellant: Sullivan Breen King Defence, St. John's; Spiteri & Ursulak, Ottawa.

Solicitor for the respondent: Department of Justice & Public Safety, Special Prosecutions Office, St. John's.

Solicitor for the intervener Director of Public Prosecutions: Public Prosecution Service of Canada, Toronto.

Solicitor for the intervener Attorney General of Ontario: Crown Law Office, Criminal, Toronto.

Solicitor for the intervener Director of Criminal and Penal Prosecutions: Director of Criminal and Penal Prosecutions, Quebec City.

Solicitor for the intervener Attorney General of British Columbia: Ministry of Attorney General, Criminal Appeals and Special Prosecutions, Victoria.

Solicitor for the intervener Attorney General of Alberta: Justice and Solicitor General Appeals, Education & Prosecution Policy Branch, Calgary.

Solicitors for the intervener Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic: Presser Barristers, Toronto; Markson Law Professional Corporation, Toronto.

Solicitors for the intervener Canadian Civil Liberties Association: Addario Law Group, Toronto.

Solicitors for the intervener Criminal Lawyers' Association: Stockwoods, Toronto; Ruby, Shiller & Enenajor, Toronto.

Solicitor for the intervener Canadian Association of Chiefs of Police: Royal Newfoundland Constabulary Legal Services Unit, St. John's.