The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference

Volume 94 Article 10

2020

A Comment on R. v. Reeves: Investigative Issues with Shared Electronic Devices and Data

Mabel Lai
Ministry of the Attorney General (Ontario), Crown Law Office — Criminal

Citation Information

Lai, Mabel. "A Comment on R. v. Reeves: Investigative Issues with Shared Electronic Devices and Data." *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 94. (2020).
https://digitalcommons.osgoode.yorku.ca/sclr/vol94/iss1/10

This Article is brought to you for free and open access by the Journals at Osgoode Digital Commons. It has been accepted for inclusion in The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference by an authorized editor of Osgoode Digital Commons.

A Comment on *R. v. Reeves*: Investigative Issues with Shared Electronic Devices and Data

Mabel Lai*

I. OVERVIEW

Digital privacy is the shared intellectual playground of the legal and technological cognoscenti. Although our legal traditions have been slow to adapt to our technological reality,[1] they *are* adapting — and the imperatives of modern policing must adapt in tandem. That need is keenly felt in respect of the Supreme Court of Canada's adaptation, in *R. v. Reeves*,[2] of our traditional concepts of ownership and privacy to the arena of shared electronic devices and data.

It is an old problem applied to a new context: when the courts speak, the police must react. Immediately. As every responsible police service is aware, complacency in the face of legal developments can have dire consequences for ongoing investigations.[3] But concrete guidance is not

---

* Crown Counsel, Ministry of the Attorney General (Ontario), Crown Law Office — Criminal. The views expressed in this paper are those of the author and not of her employer.

1 See S. Magotiaux, "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015) 71 S.C.L.R. (2d) 501-515; G. Chan, "Text Messaging: The Most Private (And Recorded) Form of Communication", *The Advocates' Journal* (2018) 36 Adv. J. No. 4 26-29.

2 [2018] S.C.J. No. 56, 2018 SCC 56 (S.C.C.).

3 See, for example, the dissenting reasons in *R. v. G.T.D.*, [2014] A.J. No. 879, 2017 ABCA 274, at para. 90 (Alta. C.A.), rev'd [2018] S.C.J. No. 7, 2018 SCC 7, [2018] 1 S.C.R. 200 (S.C.C.):

> Relying on a precedent with deep roots in Canadian law is understandable, but police services have an ongoing obligation to consider whether their practices have kept pace with developments in *Charter* jurisprudence. Changes in the law may require the police to re-evaluate their historic practices. Rather than waiting for a binding appellate decision that specifically approves or disapproves of a policy or procedure, police services should consider how courts are likely to apply settled *Charter* principles, and reasonably anticipate how broad statements of law might require changes to their traditional practices. It is particularly important for the police to respond to developments in the law when a practice — like a standard police caution - may affect many individuals' *Charter* rights.

always available in the fraught and fledgling area of digital privacy. Like the technologies underlying the debate, the law is a logic-driven exercise beleaguered by an inherent uncertainty in its application. The normative approach to defining reasonable expectations of privacy is fundamentally aspirational and therefore laden with value judgments that enhance predictive uncertainty.[4] And unlike the jurists, counsel and academics who have devoted energies to unpacking the potential applications of section 8 Charter jurisprudence to our technological reality, criminal investigators will not usually have the luxury of contemplative reflection and protracted debate before deciding on a course of action.

The past decade's worth of section 8 Charter litigation demonstrates the manner in which competing views on digital privacy can be reasonably held and powerfully defended, sometimes for years, until the question is resolved in the Supreme Court of Canada.[5] The resulting flux in the legal landscape is inevitable, and on balance, desirable. There is much to commend the appellate process as a mode of jurisprudential development. However, the attendant uncertainty has significant implications for the day-to-day conduct of criminal investigations.

This article considers some of those implications. The first section explores the baseline from which post-*Reeves* investigative action must begin. The second section considers two questions explicitly left open in *R. v. Reeves*. The third section posits additional scenarios in which *R. v. Reeves* will impact the investigation of technology-assisted or technology-targeted crime.

II. LESSONS

1. The Background

The factual simplicity of *Reeves* belies its legal complexity. Mr. Reeves was charged with assaulting his common-law spouse, Ms. G. A court order

---

Of course, the police are not allowed to simply choose the least onerous path through a constitutional gray area: *R. v. Fearon*, [2014] S.C.J. No. 77, 2014 SCC 77, [2014] 3 S.C.R. 621, at para. 94 (S.C.C.).

[4] For a succinct explanation of the normative approach, see S. Coughlan, "Grappling with Normative Notions of Privacy: *R. v. Mills*" (2019) 54 C.R. (7th) 61.

[5] If we start the clock from *R. v. Morelli*, [2010] S.C.J. No. 8, [2010] 1 S.C.R. 253 (S.C.C.), establishing, in the context of a carelessly drafted, misleading and incomplete Information to Obtain a search warrant, that "it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer" (paras. 105-106), the examination of which can reveal "the electronic roadmap of your cybernetic peregrinations" (para. 3).

prohibited him from being in the family home without Ms. G's written revocable consent. Ms. G initially provided that consent. She revoked it in a phone call to Mr. Reeves' probation officer. She expressed safety concerns. She wanted to leave the relationship. She and her sister, who had lived in the home for a period, had found approximately 30 movies of child pornography on the family computer. Her sister confirmed to the probation officer that one of the videos was entitled "11 and 12 year-old doing daddy". Ms. G and Mr. Reeves's teenage daughters lived in the family home.

Mr. Reeves was in bail court when the contraband came to light. The probation officer told Ms. G not to move the computer, and that she would call the police. Ms. G did not object. The probation officer called the local Crown Attorney's office and the police. A police officer attended the home. Ms. G invited him inside. Ms. G and her sister told the officer that Mr. Reeves had recently tried to wipe the computer clean.

Ms. G signed a written consent to allow the officer to seize the computer.[6] The officer waited for Ms. G to bring him the computer. He did not search the home. He did not turn on the computer. He did not inspect any of the data on the computer. He seized the computer pending a search warrant to re-seize it from property and to examine its contents. He inadvertently failed to file a Report to Justice pursuant to section 489.1 of the *Criminal Code*[7] until after that search warrant was issued, about four months later. The authorized examination revealed 140 images and 22 videos of child pornography, and a Bit Torrent file with video titles suggestive of pre-pubescent incest.

2. The Procedural History

The trial judge held that Ms. G could neither consent to the officer entering the family home, nor to the officer seizing the family computer. In his view, *R. v. Cole* required that the officer obtain the consent of every person who had a privacy interest in the home and computer.[8] The trial judge found Mr. Reeves's section 8 Charter rights were infringed by this conduct, as well as by deficiencies in the search warrant and the delayed

---

[6] There was a factual dispute about the validity of this consent. At trial, Ms. G. testified that she did not think she had a choice whether to sign the form: *R. v. Reeves*, [2018] S.C.J. No. 56, 2018 SCC 56, at para. 46 (S.C.C.).

[7] R.S.C. 1985, c. C-46.

[8] Interestingly, the trial judge also presided over the trial in *R. v. Cole*, [2012] S.C.J. No. 53, 2012 SCC 53, [2012] 3 S.C.R. 34 (S.C.C.).

filing of the report to justice. He made strong findings about the nature of the police conduct. He excluded the child pornography under section 24(2).

The Crown appealed against the acquittal. A unanimous Court of Appeal for Ontario allowed the appeal, holding that Ms. G had the authority to consent to the officer's entry into the family home and to the seizure of the family computer. They relied on a multitude of factors that established that Ms. G and Mr. Reeves had equal and overlapping privacy interests in the home, where they lived with their teenage daughters, and in the family computer, which had a "general password that is just open so that anybody can use it" and was regularly used by any member of the family.[9] Although the deficiencies in the search warrant gave rise to a section 8 Charter breach, the child pornography should not have been excluded under section 24(2).

3. The Decision of the Supreme Court of Canada

Mr. Reeves successfully appealed to the Supreme Court, with leave, from the decision of the Ontario Court of Appeal. The Supreme Court allowed the appeal, excluded the evidence, and restored the acquittal. The result was unanimous. The reasoning was not. Writing for the majority, Karakatsanis J. expressly declined to address whether the entry into the family home was lawful.[10] On the "assumption" that the entry was lawful, "third party consent" could not authorize the seizure of the shared device. A user of that device maintains a reasonable expectation of privacy in the device that cannot be nullified or waived by another user who shares control. Ms. G's consent was therefore insufficient authority for the warrantless seizure of Mr. Reeves's computer.[11] There was no other source of authority available to the officer, who did not believe that he had reasonable grounds to effect that seizure. The majority also declined to resolve whether section 8 of the Charter is

---

[9] *R. v. Reeves*, [2017] O.J. No. 3038, 2017 ONCA 365 (Ont. C.A.) [*Reeves* (OCA)]. The relevance of Mr. Reeves's court-ordered inability to access the family home and computer to his reasonable expectation of privacy was the subject of reasoned debate at all levels of court. There is a self-evident incongruency in relying on state-compelled conduct or a state-generated state of affairs as a basis for undermining an expectation of privacy that would otherwise have availed: see, for example, *R. v. Reeves*, [2018] S.C.J. No. 56, 2018 SCC 56, at para. 38 (S.C.C.), citing *R. v. Marakah*, [2017] S.C.J. No. 59, 2017 SCC 59, [2017] 2 S.C.R. 608, at para. 130 (S.C.C.).

[10] At the hearing of the appeal, counsel for Mr. Reeves did not challenge the entry to the home, and counsel for the Crown conceded the deficiencies in the search warrant: *R. v. Reeves*, [2018] S.C.J. No. 56, 2018 SCC 56, at paras. 15, 72-75 (S.C.C.).

[11] *R. v. Reeves*, [2018] S.C.J. No. 56, 2018 SCC 56, at paras. 20-26, 62 (S.C.C.).

engaged if an individual voluntarily brings or offers an item to the police (as opposed to the police taking it from the individual on consent).

In his concurring opinion, Moldaver J. was of the view that the Court should address the legality of the police entry into the family home.[12] He posited the ancillary powers doctrine as "a possible alternate" basis for lawful entry into the family home, and provided five tentative criteria for a common law power to enter a shared residence to take a statement.[13]

In separate concurring reasons, Côté J. opined that a co-habitant could consent to police entry into the common areas of the family home. She accepted that the police had a common law power to enter a shared residence to take a statement, but would have further held that individuals with overlapping privacy interests and rights in a common space can permit entry by a third party, police or otherwise. In so doing, the co-habitant was waiving their own right — no one else's. Justice Côté would have also affirmed the lawfulness of the police seizure of the family computer. Mr. Reeves's expectation of privacy was attenuated by the realities of joint ownership and joint use, such that Ms. G could consent to a seizure of the physical device — albeit not the data that resided on it.

4. The Takeaways

Despite the parties' mixed success in the courts below, the majority of the Supreme Court held that the police should have known that Ms. G's consent was insufficient authority for the seizure of the family computer.[14] That point was arguable before the decision; it is not now. Indeed, three propositions appear beyond dispute after *R. v. Reeves*. First, the police cannot seize a shared electronic device based on the consent of a

---

[12] It is interesting that the majority did not share this view, given the highly contextual and fact-specific inquiry into the *existence* of an expectation of privacy for the purposes of s. 8 of the Charter, and the important role that the *nature and extent* of that expectation plays in the analysis under s. 24(2) of the Charter. It may be that the impact on the Charter-protected informational interest was so great that, as a practical matter, the territorial interest had no role left to play.

[13] *R. v. Reeves*, [2018] S.C.J. No. 56, 2018 SCC 56, at paras. 71-99 (S.C.C.). The criteria are summarized at para. 96.

[14] This reasoning is reminiscent of how "genuine ambiguity" for the purposes of statutory interpretation does not arise from the existence of more than one possible interpretation, or because lower courts or doctrinal writers have come to different conclusions: *R. v. Bell ExpressVu Limited Partnership*, [2002] S.C.J. No. 43, [2002] 2 S.C.R. 559, at para. 30 (S.C.C.); *Canadian Oxy Chemicals Ltd. v. Canada (Attorney General)*, [1998] S.C.J. No. 87, [1999] 1 S.C.R. 743, at para. 14 (S.C.C.); *Sullivan on the Construction of Statutes*, 5th ed. (Markham: LexisNexis Canada, 2008) at 12-18.

proper subset of its users.[15] Second, the police cannot examine the data on a shared electronic device based on the consent of a proper subset of its users. Third, the police cannot ask a user of a shared electronic device to show them the data on it, or conduct themselves in a manner that is tantamount to asking.

Although the consent of a proper subset of users is insufficient authority to seize a shared device, the police may still rely on other sources of lawful authority, such as the plain view doctrine, exigent circumstances, search incident to arrest, or the ancillary powers doctrine. Recall that the officer in *Reeves* did not subjectively believe that a child pornography offence had been committed and that the shared device would afford evidence of that offence, although he had a clear objective basis for that belief. On a different record, sources of authority apart from consent would have been ripe for consideration.

A less dramatic but equally important takeaway is the constitutional importance of section 489.1 of the *Criminal Code*. In her concurrence, Côté J. emphasized the importance of the reporting requirement as a gateway to the statutory protections conferred on persons whose things have been seized.[16] Law enforcement in Ontario were put on notice about this issue almost four years ago in *R. v. Garcia-Machado*.[17] Law enforcement across the country now must also take heed.

III. Two open Questions

1. Entry into a Shared Home to Seize a Thing

The Court explicitly diverged on two questions. The first question was if and when a co-habitant could consent to police entry into a shared home to seize an electronic device.

Section 487 of the *Criminal Code* contemplates authority to search a place, for a thing — and then the seizure of the thing, from that place. The Supreme Court of Canada's seminal decision in *R. v. Vu*, addressing the requirements of a computer search warrant, put to bed any dispute about the privacy interests implicated by the examination of data on an electronic device, and the need to write to those interests in the search

---

[15] A proper subset is a subset that is strictly contained in the set, and therefore necessarily excludes at least one member of that set.

[16] *R. v. Reeves*, [2018] S.C.J. No. 56, 2018 SCC 56, at para. 134 (S.C.C.).

[17] [2015] O.J. No. 4146, 2015 ONCA 569, at para. 55 (S.C.C.).

warrant application.[18] But *R. v. Vu* also escalated an ongoing debate about whether an electronic device is the "place" to be searched or the "thing" to be seized, for the purposes of section 487 of the *Criminal Code*.[19] The current approach in Ontario is to describe the physical location from which the device will be seized as the "place", and to describe the device as the "thing" to be seized from that place. Terms and conditions are included in the search warrant to circumscribe the examination of the data contained in or available to the device, and to ensure that the overall search is no more intrusive than is reasonably necessary.[20] In short — and despite the frequent use of the phrase — one does not truly "search" a computer. One searches a physical location for the computer, seizes the computer, and then examines the data contained in or available to the computer, subject to certain limiting terms and conditions.

The distinction between the search of the "place", the seizure of the "thing", and the examination of the data on or available to the "thing" is important. For example, places can only be entered, and things can only be seized, during the timeframe of execution identified in the search warrant. But things can be examined at any time subsequent to their seizure — and with an electronic device, the examination of the data contained on or available to it is the kernel of the privacy complaint. Each of these investigative stages has its own implications for privacy and for the section 8 Charter analysis. The analysis in *R. v. Morelli* is an example of those distinct stages translating into distinct features of the impugned act: the constitutional wrong was that the police *searched* a home (place), *seized* a personal computer from it (thing), and then *examined* the data contained on it "without supervision or constraint" — all without lawful authority.[21]

In contrast, the majority in *Reeves* did not find it necessary to address whether the police were lawfully in the shared living room (place). The analysis in *Reeves* characterizes the constitutional wrong compendiously: that the police seized a home computer without lawful authority. Whether the territorial privacy interest in the shared living room was infused into

---

[18] *R. v. Vu*, [2013] S.C.J. No. 60, [2013] 3 S.C.R. 657 (S.C.C.).

[19] Or its analogues. The court in *Vu* compared a computer to other "places" (quotation marks in original).

[20] See, for example, the manner of execution discussion in *R. v. John*, [2018] O.J. No. 4495, 2018 ONCA 702, at paras. 16-26 (Ont. C.A.). Section 487(2.1)(a) of the *Criminal Code* addresses data contained in or available to the computer system.

[21] *R. v. Morelli*, [2010] S.C.J. No. 8, [2010] 1 S.C.R. 253 (S.C.C.). Deficiencies in the drafting of the Information to Obtain resulted in the quashing of the search warrant for Mr. Morelli's home and the seizure and examination of his computer.

or subsumed by the informational interest in the data residing on or available to the computer is unclear. However, *Reeves* should not be taken as depriving future courts of the ability to fully consider the manner, including the location or the specific device, from which the thing was seized or the data was accessed or examined.[22] For example, "Does X have a privacy interest in her banking information" is a question wrongly asked, because it lacks section 8 Charter meaning without additional context. It is one thing if the banking information is accessed through an electronic copy posted to her public Instagram profile, another if it is accessed through an electronic copy stored on the servers at her bank, and quite another if it is accessed through an electronic copy stored on the computer in her bedroom.

Further, the majority in *Reeves* does not provide separate roles for the seizure of the "thing" (for which the police relied on consent), and the examination of the data contained on that "thing" (for which the police did not rely on consent, and obtained a search warrant). Privacy is contextual; the location from which the device was seized, and the precise nature of the privacy intrusion engaged by the seizure, should be given distinct and full consideration. As Côté J. pointed out in her concurring reasons, it is important to be precise about the privacy interests that are implicated by a seizure of a computer as opposed to an examination of its contents.[23] The informational privacy interests at the forefront of the majority's analysis are engaged by the data, and either not at all or to a lesser degree by the device itself. Consider if the computer in *Reeves* only had evidentiary value as a physical object (*e.g.*, as property obtained by crime, or as a substrate for fingerprints or DNA). A proper analysis would account for the reason for which the police actually *sought* the computer — as an object, or as a data storage medium — and how the police actually *acted* in relation to that computer. The majority decision in *Reeves* should not be taken as preventing the police, in an appropriate case, from taking custody of an electronic device (*i.e.*, acting on it as an object), pending a search warrant

---

[22] Consider, for example, the question left open in *R. v. Marakah*, [2017] S.C.J. No. 59, 2017 SCC 59, [2017] 2 S.C.R. 608 (S.C.C.) about the place of the search — whether it was the device through which the messages were accessed or stored, or in a "metaphorical chat room". While the manner of access may not have been relevant to resolve the question of standing, it should remain relevant to the resolution of any substantive section 8 Charter inquiry.

[23] Further to the terminological debate described earlier, Côté J. writes of "a *search* of its contents" (emphasis in original) (para. 106).

to permit the examination of its data (*i.e.*, acting on it as a data storage medium).[24]

This shift in the Court's analytical lens — through which it was not necessary to give effect to the territorial interests or the distinction between the seizure of the device and the examination of the data contained on it — underscores the increasing importance of informational privacy in the section 8 Charter landscape.[25] In the end result, there remains a persuasive line of authority that the police may enter and examine a common area of a shared home, based on the consent of a co-habitant. Entry into and seizures from the common area of the family home could engage different considerations than entering and seizing that same item from a bedroom or other private area of that same home.[26] However, venturing any further into the home entails a significant litigation risk.[27]

2. Voluntary Surrender of a Thing to the Police

The second question is if and when a voluntary surrender of an electronic device to the police engages section 8 of the Charter. The distinction between a surrender and a solicited but valid consent is unclear.

In dismissing the Crown's policy argument that accepting Mr. Reeves's position would prevent victims of harassing or threatening text messages

---

[24] The majority explicitly contemplates relying on the doctrine of exigent circumstances as authority for preservation. It may be that less onerous requirements may suffice. Consider the line of authority in Ontario holding that mere sealing of hospital blood samples, pending a search warrant, is not an unreasonable seizure: *R. v. LaChappelle*, [2007] O.J. No. 3613, 2007 ONCA 655, at paras. 29, 41 (Ont. C.A.), leave to appeal to S.C.C. refused [2007] S.C.C.A. 584; *R. v. Gettins*, [2003] O.J. No. 4758, 181 C.C.C. (3d) 304 (Ont. C.A.); *R. v. O'Brien*, [2007] O.J. No. 771, 2007 ONCA 138 (Ont. C.A.).

[25] See *R. v. Spencer*, [2014] S.C.J. No. 43, [2014] S.C.R. 212, 2014 SCC 43, at paras. 34-51 (S.C.C.), in which Cromwell J. provides guidance on the conceptual framework and content of informational privacy.

[26] As a practical matter, reliance on consent as authority for the seizure of an electronic device poses challenges, such as the high standard to demonstrate waiver, the difficulty in precisely articulating the scope of an anticipated examination of the data residing on or available to the device, and the right of the claimant to revoke their consent at any time. Consider, for example, the potential issues arising from the examination of a sexual assault complainant's electronic device, and the possibility that the data therein could constitute a "record" for the purposes of the third party records regime in ss. 278.92-94 of the *Criminal Code*.

[27] Rather than reproduce it in this paper, please see the detailed discussion and cases cited by the Crown in its Respondent Factum before the Supreme Court at pp. 9-26: online: <https://www.scc-csc.ca/WebDocuments-DocumentsWeb/37676/FM020_Respondent_Her-Majesty-the-Queen.pdf>.

from showing those messages to the police, the majority noted that "the issue of whether s. 8 of the *Charter* is engaged when a private citizen *offers* information or an item to the police in which another person may have a reasonable expectation of privacy does not arise in this case", and contemplates a different result had Ms. G voluntarily brought the computer to the police.[28]

As Côté J. observed, the result risks "an unworkable doctrine whereby a joint owner/user of an object could voluntarily give the object to the police but could not consent to an affirmative request to seize it. Delineating the boundaries of such a distinction would be a difficult task; and in any event, it would amount to a distinction without a difference."[29] The majority's concern is with the co-user's *information* — and with it falling into state hands without his consent. If another citizen turns the shared device over to the state, the interference with the co-user's informational interests is no different, and the co-user's "loss of control over the subject matter" is no more voluntary than was Mr. Reeves's when Ms. G. revoked consent and the court order operated to separate him from the shared device.

Further, the majority's reasoning contemplates a witness being permitted to *describe*, but not *show*, data on a shared device to the police, with the description forming the grounds for lawful authority to examine that data.[30] A simple hypothetical demonstrates the practical challenges in giving effect to this distinction. Consider a complainant who brings a shared tablet to the police station. She wants to report child sex abuse material on that tablet. She tries to show the police a video. The police stop her. Pursuant to *R. v. Reeves*, they say they cannot look at the screen, but they can hear her description of what is on it. Can the complainant watch the video or refresh her memory from it from time-to-time as needed — or is that the functional equivalent of the police looking at it themselves? Can the police ask clarifying questions, and if so, is the complainant entitled to manipulate the device in order to answer those questions? Is there a difference if the complainant came to the police station with hard-copy screen-captures of what she observed? What if the complainant is a young person or has a unique vulnerability, such as particular mental illnesses or communication disorders?[31] Is there a

---

[28] *R. v. Reeves*, [2018] S.C.J. No. 56, 2018 SCC 56, at para. 46 (S.C.C.).

[29] *Id.*, at para. 129 (S.C.C.).

[30] *R. v. Marakah*, [2017] S.C.J. No. 59, 2017 SCC 59, [2017] 2 S.C.R. 608, at para. 50 (S.C.C.) ("will typically permit the police to obtain a warrant").

[31] *Id.*, at para. 183.

threshold at which the police are entitled or obliged to look at the video, to satisfy themselves of the reliability of the complainant's report — and would that action be curable by disclosure in the Information to Obtain (*e.g.*, as information known but not relied upon)? What if the complainant does not want to look at or describe the video in words? What if the complainant is the victim of the activity — is it a constitutional imperative that she describe the video of herself to the police, though it may further enhance the risk of re-victimization inherent in the investigation and prosecution of offences of that nature?

A partial solution avails if *Reeves* is strictly confined to the situation that all three opinions sought to address: the shared device. The majority decision in *Reeves* should not be taken to apply to solely-used devices — as will hopefully be the case in most child exploitation, sexual violence or intimate-partner violence investigations. Neither should the majority decision in *Reeves* be taken as resolving the policy concerns raised by Moldaver J. in his dissent in *Marakah* about a complainant's ability to consent to the police accessing a text message conversation through his solely-used device. *Marakah* established that Mr. Marakah had standing to challenge the admissibility of his electronic conversation with Mr. Winchester, though it was accessed through Mr. Winchester's device. *Reeves* is silent on whether Mr. Winchester's consent would have been sufficient authority for the police to view that electronic conversation, if it was accessed through Mr. Winchester's device. The proper interaction of *Marakah* and *Reeves* is not yet settled, and the current state of the law provides no reason to adopt a categorical approach for solely-used devices — particularly where the text messages are themselves the *actus reus* of an offence (*e.g.*, luring, threatening, criminal harassment), or where the relationship is readily demonstrated to fall outside the scope of section 8 Charter protection.[32]

IV. WHAT THE FUTURE MAY HOLD

Questions remain about the contours of legitimate investigative conduct with respect to shared devices, and will continue to arise as the jurisprudence develops around informational privacy in the context of technology-assisted crime.

The Court will have to grapple with what constitutes a "shared device" or "shared data" — from banal technologies like a shared

[32] *R. v. Mills*, [2019] S.C.J. No. 22, 2019 SCC 22, at paras. 24-26 (S.C.C.).

voicemail account, to shared private spaces like an online portal for a joint bank account, to shared public spaces abstracted from identifiable devices or parties like a hacking forum on the dark web.[33] The use of online or other electronic undercover techniques also raises the question whether an electronic communication can be characterized as a "shared space" (or metaphorical chat room, to borrow the phraseology from *Marakah*), and whether the consent of one party is sufficient authority for its examination by law enforcement.[34] Recent decisions — *R. v. Mills*,[35] *R. v. Bearisto*,[36] and *R. c. Blais*[37] — suggest that the holding in *Reeves* may have limited applications to these undercover scenarios.

The impact on *R. v. Reeves* in the context of technology-targeted crime is also a live issue. Sophisticated cybercrime attacks (*e.g.*, DDOS, hacking, ransomware, malware) will target infrastructure, large-scale commercial operations, financial and educational institutions, and governmental operations.[38] The targeted technology will necessarily implicate the private data of hundreds of thousands, if not more, of individuals who may or may not reside in Canada. It will not be feasible for the police to identify, much less obtain consent, from all those individuals. Recall that the majority in *R. v. Reeves* would have required a search warrant to simply seize the device, before any examination of the data on it. Corporations and institutions will not wait for a search warrant to seize or lock down their servers; they will take immediate action to rectify any data breach and mitigate the financial and public relations impact, even if that contaminates the forensic trail. It remains to be seen whether law enforcement can have recourse to institutional or corporate consent, exigent circumstances, plain view, the ancillary powers doctrine, or some other source of warrantless authority to

---

[33] Consider, for example, *R. v. Anstie*, [2019] O.J. No. 806, 2019 ONSC 976 (Ont. S.C.J.) (crash data recorder in rental car is not analogous to the shared device in *Reeves*, "but more importantly, it is the nature of the data itself" that renders it "unable to give rise to s. 8 protection").

[34] *R. v. Marakah*, [2017] S.C.J. No. 59, 2017 SCC 59, [2017] 2 S.C.R. 608, at para. 30 (S.C.C.).

[35] [2019] S.C.J. No. 22, 2019 SCC 22 (S.C.C.).

[36] [2018] A.J. No. 379, 2018 ABCA 118 (Alta. C.A.), leave to appeal to SCC refused [2018] S.C.C.A. No. 188.

[37] [2017] J.Q. no 15774, 2017 QCCA 1774 (Que. C.A.), leave to appeal to SCC refused [2018] S.C.C.A. No. 132.

[38] See, for example, Royal Canadian Mounted Police, "Cybercrime: an overview of incidents and issues in Canada" online: <http://www.rcmp-grc.gc.ca/wam/media/1090/original/ea3c6b40418cad578c40d403b24cda43.pdf> (published in 2014); also the Reports and Assessments available for public consumption on the Canadian Centre for Cyber Security website, online: <https://cyber.gc.ca/en/reports-assessments>.

forensically image, seize or otherwise preserve the targeted technology for investigation.

It is difficult to predict the emergence of new technologies, let alone the role they will play in our daily lives. It is no easier to predict how the law will adapt to meet those technological developments. The only certainty is that the legitimate dictates of public safety and constitutional norms will continue to interact with each other in a complicated dance through the jurisprudence, for many years to come.