Is a Subsequent Report to a Justice Required for the Seizure of Data Under the Section 489.1 Regime?

DEREK ZAPORZAN *

ABSTRACT

Section 489.1 of the *Criminal Code* requires the police to report to a justice anything that they have seized in the execution of their duties. Failure to do so will often constitute a breach of s. 8 of the *Charter*, possibly resulting in the exclusion of evidence under s. 24(2). The Supreme Court of Canada has yet to provide any direction on whether s. 489.1 applies to the extraction of data from an accused's electronic device specifically, or to the collection of electronic data more broadly. In the absence of such guidance, provincial courts have conducted their own analyses on this issue and have come to completely opposite conclusions.

This paper first considers the common-law and statutory roots of this reporting regime, along with its public policy objectives and practical limitations. It then examines recent Supreme Court decisions that have recognized heightened privacy interests in informational privacy. The analysis proceeds to a review of recent divergent case law from Ontario, Saskatchewan, British Columbia and Alberta on this very issue, ultimately

* The author is currently a third-year Juris Doctor candidate at the University of Manitoba and has been a Police Officer with the Winnipeg Police Service since 2006. The author would like to thank Professor John Burchill for his guidance, the student editor at the Manitoba Law Journal for their assistance, and the anonymous peer reviewers for their feedback.

concluding that s. 489.1 should not, as a general rule, require the police to report the seizure of electronic data to a justice. Finally, this paper considers whether, under the alternative conclusion, the exclusion of such evidence would be a justifiable remedy.

Keywords: *Charter; Section 8; Search and Seizure; Informational Privacy; Seizure of Data and Electronic Documents; Report to a Justice; Form 5.2; Criminal Code ss. 489.1 and 490*

I. INTRODUCTION

Section 8 may presently be the most dynamic and evolving area of Canadian *Charter*[1] jurisprudence. This is especially true with respect to informational privacy. In the past year alone, the Supreme Court of Canada released two separate decisions that clarified the way in which police can engage with electronic documents or data where an individual may have a claim to a reasonable expectation of privacy.[2] This should come as no surprise, given the ever-increasing role that technology, the internet, and electronic data play in the daily lives of Canadians.

Despite its constant expansion and refinement of informational privacy protections, the Supreme Court has been silent on whether the police are required to report to the courts whenever they seize electronic information in which an individual has privacy expectations. This paper aims to address the unresolved question of whether police must report the seizure of data from an electronic device to a justice. The provincial courts have answered this question inconsistently, and the Supreme Court has yet to provide any guidance.

The typical scenario considered in this paper is where police have seized an electronic device, such as a mobile phone or computer, during the course of an investigation. Section 489.1 of the *Criminal Code*[3] mandates that police must, using a standard form ("Form 5.2"), report the seizure of the device to a justice.[4] Case law is now sufficiently clear that police require prior

---

1 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11 [*Charter*].

2 See *R v Bykovets*, 2024 SCC 6 [*Bykovets*]; See also *R v Campbell*, 2024 SCC 42 [*Campbell*].

3 *Criminal Code*, RSC 1985, c C-46 [*Criminal Code*].

4 In this paper, both the process itself and the standard form required in that process will

judicial authorization to conduct a search of an electronic device where the claimant has a reasonable expectation of privacy,[5] barring limited circumstances.[6]

If the police have seized the device lawfully, submitted a Report to a Justice notifying the court of the seizure, and obtained prior lawful judicial authorization (i.e., a warrant) to search the device, the question becomes: Do the Police need to submit a second Report to a Justice once informational data has been collected from the device? This question raises several sub-issues:

- What is the underlying public policy objective of the statutory scheme relating to the seizure, detention and disposition of things seized by the police in an investigation?
- Is the device a "*place*" or a "*thing*"?
- Does the collection of informational data from the device even constitute a "seizure", thus engaging s. 489.1 reporting obligations?
- Can a justice properly supervise the detention of electronic data? Furthermore, in what circumstances, if any, would a justice actually return seized electronic data to a claimant or otherwise dispose of it?
- Does the failure of the police to comply with the statutory reporting requirements relating to items otherwise seized lawfully amount to a *Charter* infringement in *all* instances? And if so, what is the appropriate remedy?

This paper addresses each of these questions in turn. It concludes that, although an electronic device, such as a computer or a phone, is both a "thing" that can be seized and a "place" where further searches can occur, the extraction or duplication of data on the device does not constitute a "seizure" warranting additional reporting requirements. Accordingly, the failure to submit an additional Report to a Justice in these circumstances

---

be referred to as a Report to a Justice. The term "Form 5.2" will also be used to describe the form required.

5 See *R v Vu*, 2013 SCC 60 [*Vu*].

6 *R v Fearon*, 2014 SCC 77 [*Fearon*] explores the circumstance where a search of a device by police incident to a lawful arrest would be justified absent prior judicial authorization. Similarly, *Campbell*, *supra* note 2, applies the doctrine of exigent circumstances to justify searching a device without a warrant.

would not constitute a s. 8 breach. This conclusion is based on both public policy and practical considerations.

However, if this conclusion is incorrect, and the failure to report the seizure of data from a device to a justice does in fact violate a claimant's s. 8 *Charter* rights, it should generally be regarded as a minor administrative or technical breach, provided there is no bad faith on the part of the police. In such cases, exclusion of the evidence under s. 24(2) of the *Charter* would not be warranted.

BACKGROUND: THE COMMON LAW

Presently, many of the police's powers of search and seizure are codified by statute,[7] although this was not the case historically.[8] To understand the contemporary rationale for requiring officers to report a list of items seized in the execution of their duties, it is important to consider the historical common-law roots of this rule.

In *Entick v Carrington*,[9] the Court held that government officials, when acting in the execution of their duties, could only exercise powers that were expressly permitted by either statute or common law. Acting beyond these limits would subject the government actor to the same charges, such as trespass or assault, as any other individual.[10]

The common-law courts affirmed that police had the authority to search an individual incident to arrest and to seize property related to the offence charged. However, the courts were also critical of police in situations where they exceeded their search powers and seized property unrelated to the offence charged.[11] In *R v O'Donnell*, the court stated:

> Generally speaking, it is not right that a man's money should be taken away from him, unless it is connected in some way with the property stolen. If it is connected with the robbery, it is quite proper that it should be taken... I believe constables are too much in the habit of taking away everything they find upon a prisoner,

---

7 *Criminal Code*, *supra* note 3.

8 For an extensive overview of the common-law search powers of police, see John Burchill et al, *Ancillary Police Powers in Canada: A Critical Reassessment*, Law & Society Series (Vancouver: UBC Press, 2024) at 21-46 [Burchill et al].

9 [1765] 19 St Tr 1030, 95 ER 807.

10 Burchill et al, *supra* note 8 at 32-33.

11 *Ibid* at 33.

> which is certainly not right. And this is a rule which ought to be observed by all policemen and other peace officers.[12]

These early cases imply a common-law requirement for judicial oversight of any items seized by the police during an investigation. This duty applies irrespective of whether the initial arrest or seizure was lawfully justified.

STATUTORY SCHEME - THE *CRIMINAL CODE*

Prior to the enactment of the *Charter*, police powers regarding search and seizure were largely unregulated, aside from the search warrant regime (formerly under s. 443). The courts paid little attention to seizures, since there were few effective remedies for unlawful seizures before the *Charter* came into force.[13]

Following the proclamation of the *Charter* and the early case law that followed, Parliament proceeded to "fill the gaps" in the legislative scheme governing search and seizure.[14] The *Criminal Code* now codifies many of the search powers bestowed on law enforcement, though not all. For example, one holdover from the English common law, which has not been codified, is the lawful authority for police to search an individual incident to a lawful arrest.[15] The courts have recognized that these warrantless personal searches constitute the majority of searches conducted by police.[16]

Section 487 of the *Criminal Code* outlines the requirements for police to seek and execute a search warrant. Section 487.11 creates an exception to the warrant requirement where exigent circumstances make it impracticable to obtain prior judicial authorization.[17] Section 489(1) authorizes police, while executing a search warrant, to seize items not explicitly noted in the warrant where there are reasonable grounds to believe the items have been obtained by, or used in, the commission of an offence, or may provide evidence in respect of an offence contrary to any Act of

---

12 [1835] 7 Car & P 138, 173 ER 61.

13 *R v Backhouse*, 2005 CanLII 4937 (ONCA) at para 109 [*Backhouse*].

14 *Ibid* at para 110.

15 See *Cloutier v Langlois*, 1990 CanLII 122 (SCC) where the Supreme Court recognized this common-law exception to the warrant requirement for the first time.

16 *Backhouse*, *supra* note 13 at para 111.

17 *Criminal Code*, *supra* note 3, s 487.11.

Canada.[18] Similarly, s. 489(2) grants these same warrantless seizure powers to the police when they are lawfully present in a place.[19] Sections 117.02, 117.03 and 117.04 provide additional powers to the police to seize firearms, firearm parts and ammunition in certain circumstances.[20] In short, there are a variety of situations where police have the lawful justification to conduct a search and seize property from a person, with or without a warrant, under both statute and common law.

The Law Reform Commission of Canada, in its 1986 *Report on the Disposition of Seized Property*,[21] made several recommendations relating to post-seizure procedures by police and the courts. It is important to note, however, that the Commission's primary motivation in advocating for statutory amendments was not to improve access to seized items for claimants charged with a crime, but rather to provide an effective and accessible remedy for victims of crime—through the restoration of the "takings" of an offence as soon as practicable to the person lawfully entitled to possession.[22]

Additionally, when considering whether a failure to comply with statutory reporting requirements related to the seizure of items constitutes a *Charter* infringement in its own right, the Law Reform Commission's Report offers only equivocal guidance:

> Although detention of things seized constitutes an infringement of the Charter when the authorization or execution of the initial intrusion is unreasonable, the Commission believes that *in certain circumstances* the unreasonable detention of things seized under an otherwise lawfully authorized and executed search and seizure *may* also constitute an infringement of the Charter [emphasis added].[23]

The Law Reform Commission's recommendations included an obligation on the seizing officer to compile an inventory of any items seized in the

---

18 *Ibid*, s 489(1).

19 *Ibid*, s 489(2).

20 Section 117.02(2) of the *Code* mandates that any items seized under that section shall be dealt with according to ss. 490 and 491 of the *Code*. Similarly, s. 117.04(3) of the *Code* mandates that any items seized under that section require the police to file a Report to a Justice.

21 Law Reform Commission of Canada, *Report on the Disposition of Seized Property: Post-seizure Procedures* (Ottawa: Law Reform Commission of Canada, 1986) [*1986 LRCC Report*].

22 *Ibid* at 6-7.

23 *Ibid* at 5-6.

course of an investigation – whether under the authority of a warrant or otherwise – and to bring this post-seizure report to a justice "as soon as practicable", a phrase intentionally designed to take into account the operational realities of police work.[24] This requirement was framed as an accountability mechanism for the police.[25] Many of the Law Reform Commission's recommendations are now reflected in statutory amendments to the *Criminal Code*.

The Reporting Regime: Sections 489.1 and 490 of the *Criminal Code*

Parliament has since enacted ss. 489.1 and 490 of the *Criminal Code*, which establish mandatory obligations for law enforcement and the courts. These provisions are significant as they serve as a safeguard, balancing the state's ability to seize property for law enforcement purposes against the privacy rights of citizens.[26]

Section 489.1 requires police to notify the courts whenever they seize anything under a warrant, pursuant to ss. 487.11 or 489, or otherwise in the execution of their duties.[27] The courts have held that this section applies equally to seizures authorized by warrant and those conducted under common law.[28] Section 489.1(b) states that when an item has been seized and detained, the police "shall, as soon as practicable," either "bring the thing seized before a justice... or report to the justice that the thing has been seized and is being detained...".[29] Section 489.1(3) provides that Form 5.2 shall be used for this purpose.[30]

The courts have described s. 489.1 as a "gateway" that all fruits of a search must pass through to come under the judicial supervision mandated by s. 490.[31] Since the Report to a Justice is the only means by which the

---

24 *Ibid* at 12-13.

25 *Ibid* at 10.

26 *R v Pickton*, 2006 BCSC 1098 at para 60.

27 *Criminal Code*, *supra* note 3, s 489.1.

28 *Backhouse*, *supra* note 13 at para 111.

29 *Criminal Code*, *supra* note 3, s 489.1(b).

30 *Ibid*, s 489.1(3).

31 *R v Craig*, 2016 BCCA 154 at para 159 [*Craig*].

police can notify the courts of a seized and detained item, failure to submit this report hinders the courts' ability to exercise oversight and facilitate the return of the seized items to their lawful owners when appropriate.

Section 490 establishes a comprehensive scheme for the judicial oversight of items seized and detained by the police. According to s. 490(1), a justice shall order the goods returned to the lawful owner unless the justice is satisfied that the detention of the things is required for investigative purposes, a preliminary inquiry, trial or other proceeding.[32] Section 490(2) outlines two situations where police have seized an item: (a) where a person has not yet been charged with an offence; and (b) where the person has been charged.

The first situation, described in s. 490(2)(a), applies where the police have seized an item from an individual but have not yet laid charges for an offence to which the item may provide evidence. In these circumstances, the police must report the seizure to a justice as soon as practicable. If the police wish to detain the item for longer than three months, they must submit a Report to a Justice outlining the nature of the investigation and the reasons for retaining possession of the item. This process must be repeated every three months. Pursuant to s. 490(3), if the police seek to maintain detention of the item for more than one year, they must apply to a Superior Court judge, who may order further detention of the seized item if satisfied, having regard to the complex nature of the investigation, that further detention is warranted.[33]

This first situation can arise in complex white-collar crime or fraud investigations, where police seize large volumes of documents or computer data that require in-depth examination in order to confirm what charges, if any, are justified.[34] In such cases, police must submit a new Report to a Justice every three months to maintain detention of the documents if charges have not yet been authorized. If detention is required for more than one year, an application must be made to a Superior Court judge.

Another example of the s. 490(2)(a) and s. 490(3) regime may arise where police seize a mobile phone belonging to a murder suspect who has not yet been charged. Pursuant to a warrant, police may seek to extract the contents of the device for evidence relating to the murder. Due to the

---

32 *Criminal Code, supra* note 3, s 490(1).

33 *Ibid,* s 490(3).

34 See e.g. *Winnipeg (City) v Caspian Projects Inc et al*, 2021 MBCA 33.

technical limitations of phone extraction software, police may be unable to access the contents of a specific device model until new software is made available, which could take months or even years. Due to the severity of the offence being investigated, police would need to explain to the justice (or Superior Court Judge, if required) why continued detention of the device is necessary.

The second situation (s. 490(2)(b)) applies where the police have seized an item from a person who has been charged with an offence. In these cases, only one Report to a Justice needs to be filed. This scenario typically applies to most "standard" investigations. For example, consider a situation where a suspect commits a commercial robbery. Police arrest the suspect, who is in possession of a mobile phone at the time of the arrest. Police seize the mobile phone incident to arrest with the intention of later obtaining a search warrant for its contents. In such a case, "as soon as practicable" following the arrest, the police must submit a Report to a Justice, which would include the mobile phone under the list of items seized.

A. Is a second Report to a Justice required once data is retrieved from the seized device?

In the robbery example above, police lawfully seized a phone from the suspect and reported the seizure to a justice "as soon as practicable." They later obtained and lawfully executed a warrant to search the device. The question then arises whether police must submit a second Report to a Justice for the data extracted. To answer this ultimate question, it must first be determined whether the device is properly characterized as a "place" capable of being searched, or simply as a "thing" to be seized. On this point, the available case law is sufficiently clear that it is both.

1. An electronic device as both a "thing" and a "place"

In *Vu*[35], the Supreme Court held that, because computers give rise to particular privacy interests, s. 8 requires these interests to be considered before a search occurs, rather than merely after the fact. Consequently, computers must be treated "as a separate place."[36] If police come across a computer while executing a search warrant that does not expressly authorize the search of computers, they may seize the computer and take the necessary

---

35 *Supra* note 5.

36 *Ibid* at para 51.

steps to ensure the integrity of the data. However, "[i]f they want to search the data… they must obtain a separate warrant."[37] Additionally, a warrant to search a computer does not grant the police "a licence to scour the devices indiscriminately."[38] This differs from the traditional s. 8 legal framework, which does not require police executing a search warrant at a residence, for example, to obtain prior judicial authorization to search a specific cabinet or receptacle.[39]

It is important to note that, although *Vu* characterized a computer as both a "device" that can be seized and a "place" that can be searched, it did not characterize the extraction of data from the device itself as a seizure.

This heightened privacy interest in electronic devices was further recognized in *Fearon*,[40] where the Supreme Court tailored the traditional common-law power of police to search an accused incident to arrest to govern the searching of electronic devices. These modifications ensured that the common-law power complied with s. 8 of the *Charter*, having regard to the heightened privacy interests in these devices.[41] These limitations on searching a device incident to arrest were created to ensure that police do not "rummage around the device at will."[42]

McLachlin C.J., writing for the majority, made an important distinction between cell phones as physical devices and the information stored on them, noting that only the latter attracts a heightened expectation of privacy:

> Searches that treat a cell phone (or other similar device) merely as a physical object continue to be permissible incident to arrest. For example, seizing a cell phone, searching for hidden compartments, testing that cell phone for fingerprints, or reading the identification number physically inscribed on the cell phone, do not interfere with the heightened expectation of privacy in the accessible information.[43]

---

37 *Ibid* at para 49.

38 *Ibid* at para 61.

39 *Ibid* at paras 1-2.

40 *Fearon, supra* note 6.

41 *Ibid* at paras 75-84.

42 *Ibid* at para 78.

43 *Ibid* at para 155.

However, as seen in the case of *Vu*, the Supreme Court in *Fearon* did not characterize the extraction of data from the device pursuant to a search as a "seizure."

In *R v Reeves,*[44] the accused's spouse discovered what she believed to be child sexual abuse and exploitation material (CSAEM) on a laptop she shared with the accused. She notified the police, who obtained her consent to seize the laptop. However, the police did not seek a warrant to search the computer until four months after it had been seized. Following the execution of the warrant, the police located CSAEM, and the accused was charged. The police also failed to report the seizure of the computer to a justice until nearly five months after it had first been seized.[45]

The Supreme Court ultimately held that the initial seizure of the computer without a warrant was unlawful and violated the accused's s. 8 *Charter* rights.[46] Additionally, the court found that the police's failure to report the warrantless seizure of the device until almost five months after the fact violated ss. 489.1 and 490 of the *Criminal Code* – which require that a report be made "as soon as practicable" – and constituted an additional breach of the accused's s. 8 *Charter* rights.[47] Because the accused had not been charged with any offence at the time the seizure was made, s. 490(2) of the *Criminal Code* mandated that the item could not be detained for more than three months unless a further application was made. As a result, the Supreme Court excluded the evidence under s. 24(2) of the *Charter* and restored the accused's acquittal.

The decision in *Reeves* is significant for two reasons in the context of this paper. First, the Court found that a failure to comply with the statutory reporting requirements under s. 489.1 of the *Criminal Code* may itself constitute a breach of an accused's s. 8 *Charter* rights, justifying the exclusion of evidence under s. 24(2). This point will be considered in greater detail later in this paper.

The second reason *Reeves* is important is that it follows the Supreme Court's precedent in *Vu* and *Fearon*, which established that the physical device itself can be considered a separate entity from the information stored within it. Even if the search of the contents is lawfully authorized by a

---

44 2018 SCC 56 [*Reeves*].

45 *Ibid* at paras 1-3.

46 *Ibid* at para 58.

47 *Ibid* at para 63.

warrant, an unlawful initial seizure of the physical device renders any subsequent search also unlawful.

Importantly, the majority in *Reeves* held that the subject matter of the initial (unlawful) seizure encompassed not only the computer itself, but also "the data it contained about Reeves' usage, including the files he accessed, saved and deleted [emphasis added]."[48] This determination was made with due consideration to the fact that the police could not actually search the data until they obtained a warrant to do so. In other words, the computer was not initially seized for the purpose of securing any physical evidence associated with the device itself (such as fingerprints that may be present on its surface), but rather to preserve the informational data it contained. This is true for nearly every conceivable investigation involving CSAEM or cybercrime more broadly. If that is the case, and if the officers filed an initial Report to a Justice for the seized computer (which they failed to do in *Reeves*), the question then arises: What is the rationale for submitting a second report to a justice once that data has been extracted?

B. The privacy interest is in the "raw" data itself, and not in its analysis

The courts have held that the privacy interests in data lie in the uninterpreted "raw" data itself, rather than in its subsequent analysis. Therefore, if previously extracted raw data is later re-analyzed using updated software, additional judicial oversight is not required.

This principle was addressed in *R v Nurse,*[49] where police lawfully seized BlackBerry devices belonging to two suspects in a homicide investigation. The police obtained warrants to search these devices, and while the data was initially analyzed, the extraction was limited and provided little investigative value. Approximately one year later, using updated forensic software, the police re-analyzed the data and successfully retrieved messages between the suspects that discussed their plan to kill the victim. Defence counsel argued that this second analysis, using the updated software, constituted a fresh "search" and thus required a second search warrant.[50]

The Ontario Court of Appeal (ONCA) upheld the trial judge's ruling, stating that reinterpreting data with updated software did not constitute a

---

48 *Ibid* at para 30.

49 2019 ONCA 260 [*Nurse*].

50 *Ibid* at paras 119-130.

new search requiring fresh authorization.[51] The ONCA compared this process to police re-examining seized documents in a fraud case, or sending those documents to forensic accountants for further analysis.[52] Importantly, the ONCA also stated that "[s]imilarly, with respect to blood-stained articles of clothing seized pursuant to a warrant, it would not be improper for the police to re-submit these items for further DNA testing to benefit from evolving scientific advances or improved forensic techniques."[53]

When police seize articles of clothing from a suspect, it is often for the primary purpose of submitting the clothing for forensic testing. In such instances, the characteristics of the shirt — such as its colour and the fabric — are less significant than the forensic evidence (blood, etc.) it may contain. Nevertheless, in these cases, the police are not required to report to a justice when additional evidence is found on that clothing. Of course, *Vu* holds that informational privacy on computers is substantively different from territorial or personal privacy; however, the practical questions remain: How can a justice "supervise" this type of forensic evidence, and under what circumstances could such evidence be returned to the claimant or otherwise disposed of?

Although the issue of a second Report to a Justice was not directly addressed in *Nurse*, the court's reasoning suggests that no additional report would be required. If a re-analysis of the extracted data does not constitute a new "search," then no additional "seizure" could have taken place. After all, the raw data has remained unchanged. Unfortunately, there is also no indication in *Nurse* as to whether the police submitted a second Report to a Justice after the initial extraction and unsuccessful analysis. Practically speaking, however, it raises the question of what the police could list as having been seized in such circumstances – "Indecipherable raw data presently of no evidentiary value"?

C. Does the collection of data from a device constitute a "seizure", thus engaging s. 489.1 reporting obligations?

When a person has a reasonable privacy interest in an object, or in the subject matter of state action and the information it reveals, an inspection

---

51 *Ibid* at para 132.

52 *Ibid* at para 135.

53 *Ibid* at para 139.

constitutes a "search," while taking possession of that object constitutes a "seizure."[54] Importantly, not every "search" results in a "seizure"; a seizure occurs only where the individual is further deprived of possession or control of that "thing." For example, if the police take photographs of a scene while executing a search warrant, this would not be classified as a "seizure." In such circumstances, the police are not required to report the photographs to a justice, since the claimant has not been deprived of any possessions as a result of state action.

Even when electronic devices are searched, the examination of their contents does not necessarily constitute a seizure. For example, in *Fearon*, police searched a suspect's mobile device incident to arrest. Officers are permitted to conduct a limited search of the device to locate evidence against the suspect or potential co-accused. In doing so, police are obliged – pursuant to the *Fearon* decision – to make detailed notes regarding the steps taken during the search and their observations. Presumably, police would also be authorized to take photographs of the suspect's phone screen incident to arrest. In such situations, it is generally accepted that documenting the contents of a suspect's phone through police notes or photographs does not amount to a "seizure" that necessitates separate notification to the courts.

To take this analysis one step further, consider whether the "extraction" — which may also be characterized as the "duplication," "downloading," or "copying" — of data from a device using forensic software constitutes a "seizure" in the first place. This issue is the main point of divergence between courts that have determined a second Report to a Justice is required for extracted data and those that have reached the opposite conclusion.

Section 490(13) of the *Criminal Code* explicitly authorizes a peace officer who has custody of a seized document to make and retain a copy of the document before bringing it to a justice or complying with an order to return, forfeit or dispose of it. In other words, this provision allows police to keep a copy of any seized document, even if the original document is ordered to be returned to the owner or otherwise disposed of.

The question of whether s. 490(13) authorizes police to extract data from a device and thereby circumvent the overall s. 490 oversight regime

---

54 *R v Cole*, 2012 SCC 53 at para 34 [*Cole*].

was recently decided by the British Columbia Supreme Court (BCSC).[55] This case focused on data extracted from a vehicle's Event Data Recorder ("EDR"). An EDR is akin to a plane's "black box" and is capable of recording information such as a vehicle's speed prior to a collision, whether the occupant(s) were wearing seatbelts, and whether the driver attempted to brake before the collision.[56] The court held that such data did not meet the threshold of a biographical core of personal information[57] necessary to engage a reasonable expectation of privacy and the resulting s. 8 *Charter* protections.[58] The court ultimately concluded that s. 490(13) had no application to the extraction of digital data, stating:

> [M]aking a copy of a document is distinct from extracting data from a digital device. The process of copying data creates a one-for-one replication of the data. The end product created by copying is an exact duplication of the data. Conversely, the process of extracting data involves turning the information contained on a digital device into desirable and usable information. The process of extracting may, therefore, involve filtering, aggregating, and/or re-formatting the data.[59]

The BCSC's distinction between "copying" and "extracting" in this regard highlights a fundamental flaw in the wording of the statutory provisions. When Parliament enacted these provisions, data extraction was not anticipated, just as digital privacy of this kind was not foreseen when the *Charter* came into effect. As *Charter* jurisprudence has developed, achieving coherence in applying these principles to new technologies has become increasingly difficult. The binary code, which consists of an infinite sequence of 1s and 0s, is meaningless on its own. It is only through software and proper formatting that this digital data can convey any substantive information.

Even if one does not agree with the BCSC's reasoning on this point, it is still possible to accept its ultimate conclusion that s. 490(13) does not extend to the extraction of data from a device. To interpret s. 490(13) as creating an exception to the overall ss. 489.1 and 490 reporting regime could be seen as an invitation for police to circumvent judicial safeguards

---

55 *Further Detention of Things Seized (Re)*, 2025 BCSC 1442 [*Wang*].

56 *Ibid* at paras 1-13.

57 See *R v Plant*, 1993 CanLII 70 (SCC) at 293.

58 *Wang*, *supra* note 55 at para 37.

59 *Ibid* at para 45.

governing digital privacy. Such an interpretation may also fail to withstand *Charter* scrutiny. *Vu* holds that the police are not presumptively entitled to extract digital data, regardless of whether the data extracted is later found to engage a reasonable expectation of privacy.[60]

To properly assess whether data extraction should be characterized as a "seizure," it is necessary to understand how the process operates in practice. Notwithstanding the inapplicability of s. 490(13), In most circumstances, the extraction process does not cause damage to the device itself, nor does it involve deleting any of its contents. Instead, the process is akin to downloading the contents of the device, which are then analyzed using forensic software, such as Cellebrite. Such software interprets the raw data, sorts it within specified search parameters, and generates analysis reports.[61] It is difficult to frame such actions as constituting a "seizure," given that no further deprivation of the contents of the device arises as a result of the state's action.

IS A SECOND REPORT TO A JUSTICE REQUIRED FOR THE DATA EXTRACTED FROM A DEVICE?

Presently, there is little academic or legal discussion on whether a second report is required for data extracted from electronic devices. Most commentary instead focuses on situations where an officer's failure to report the initial seizure of a device to a justice may warrant a s. 489.1-based *Charter* challenge.[62] However, the distinct question of whether a subsequent report should be required for the seized data remains largely unexplored.

Justice David M. Paciocco, who currently sits on the ONCA and holds the position of Emeritus Professor with the University of Ottawa, is widely regarded as an expert on criminal law and procedure. In his previous role as a Justice with the ONSC, Justice Paciocco disregarded non-binding case law that attempted to distinguish between the seizure of property and its subsequent detention, stating:

> [A] seizure is an ongoing state of affairs so long as the seizing party continues to deprive someone of control over something. Not only does the ordinary

---

60 *Ibid* at para 48.

61 See e.g. *R v Vye*, 2014 BCSC 93 at paras 4, 5, 18.

62 See Eric Granger, "The Report to a Justice and the Charter" (Paper delivered at the 26th Annual Criminal Law Conference, 18-19 October 2014), 2014 CanLIIDocs 33361.

> interpretation of section 8 therefore suggest that it should be interpreted to embrace the retention of seized goods, the kind of purposive interpretation favoured in Charter interpretation also supports this approach... It cannot be forgotten that retention is often ordered to enable ongoing investigation relating to seized items, investigating that can constitute an ongoing search.[63]

He further emphasized that "[i]f the continuation of a seizure is not lawful, the seizure becomes unreasonable contrary to section 8 of the Charter."[64]

Interestingly, these comments arose in a case where police seized a computer hard drive suspected of containing CSAEM. The initial seizure was conducted without a warrant, and no Report to a Justice was filed. The police claimed that the warrantless seizure was necessary to preserve evidence; however, Justice Paciocco deemed the seizure unlawful. Within 13 days, investigators obtained a warrant to search the computer hard drive and subsequently reported the data seized from it to a justice. In other words, although the initial seizure of the computer was not reported, the data that it contained was reported shortly thereafter. Justice Paciocco held that this subsequent reporting of the data seized did not "cure" the initial failure to report the warrantless seizure, as the report that was eventually submitted made no mention of the initial unauthorized (and unjustified) hard drive seizure.[65]

Unfortunately, Justice Paciocco did not provide commentary on the necessity or rationale for filing a subsequent report for the data seized from a device. However, some insight may be gleaned by considering his suggested "purposive" interpretation of the *Charter*.

The Supreme Court's jurisprudence on s. 8 has consistently affirmed that the rights against unreasonable search and seizure must receive a broad and purposive interpretation:

> Section 8 of the Charter guarantees a broad and general right to be secure against unreasonable searches and seizures which extends at least so far as to protect the right of privacy from unjustified state intrusion. Its purpose requires that unjustified searches be prevented. It is not enough that a determination be made, after the fact, that the search should not have been conducted.[66]

---

63 *R v Butters*, 2014 ONCJ 228 at para 54 [*Butters*].

64 *Ibid* at para 55.

65 *Ibid* at para 56.

66 *Hunter et al v Southam Inc*, 1984 CanLII 33 (SCC) at 146 [*Hunter v Southam*].

More recently, the Supreme Court has confirmed that the broad and purposive approach applies to informational privacy. Echoing its earlier decision in *Hunter v Southam*, the Court emphasized that "s. 8 seeks to prevent breaches of privacy, rather than to condone or condemn breaches based on the state's ultimate use of that information." This is because "[p]rivacy, once breached, cannot be restored."[67]

This concern appeared central to Justice Paciocco's reasons in *Butters*. When a device is seized without prior judicial authorization and no Form 5.2 is submitted, there is no judicial record indicating that any item has been seized. As a result, the court is unable to exercise its oversight function or intervene to prevent privacy breaches before they occur. This analysis suggests that, had the officer in *Butters* submitted a Form 5.2, the Justice might have ruled the initial seizure unlawful and ordered the hard drive returned to the claimant. Such an order would have prevented any subsequent privacy breaches – specifically, the search of the hard drive pursuant to the warrant.

The practical significance of these concerns about judicial oversight is reinforced by empirical evidence. A 2017 Manitoba study examined 100 judicial authorizations for substantive and technical compliance to determine whether they should have survived *Charter* scrutiny. The findings revealed that among the authorizations requiring the submission of a Form 5.2, only 60% were submitted to the court. Additionally, of those that were filed, several contained technical errors, including incorrect warrant section numbers and incomplete reports.[68]

The absence of reports in 40% of the examined authorizations raises concerns about the court's ability to fulfill its oversight function and is indicative of systemic issues. Additionally, the study did not examine situations where reports should have been filed for seizures made without prior judicial authorization, such as those incident to arrest, although it is likely that compliance in this regard would be equally deficient.

The requirement for police to report the seizure of data from a device that has already been lawfully seized, reported, and authorized for search remains unclear, even with a broad and purposeful interpretation of the *Charter*. One potential concern is police overreach - officers may exceed the

---

67 *Bykovets, supra* note 2 at para 6.

68 Anne Krahn et al, "Reaching For Excellence: Evaluating Manitoba's Process For Issuing Judicial Authorizations" (2017) 40:1 Man LJ 41 at para 82.

limits set by the issuing Justice when executing the search warrant. These limits can include specific restrictions on the types of files that may be searched. For example, a Justice may order that only text messages from a device can be extracted, but not photographs. Additionally, there may be restrictions on the dates for when files were sent or received. For example, a Justice could order the device to be searched for "text messages exchanged between the accused and Person X between the dates of January 1st and 14th, 2023." Any data obtained outside of these search parameters would be prima facie unlawful.

Such an obvious disregard of judicial authority by the police would almost certainly result in the exclusion of any additional evidence gathered. It is unlikely that requiring a Form 5.2 to be submitted in such a circumstance would do anything further to dissuade such conduct. Based on the 2017 Manitoba study, even if a Form 5.2 were to be submitted honestly, there's still no guarantee that the court would identify the police overreach at that stage. This weighs against the argument that requiring a Form 5.2 in such circumstances supports the purposive approach to s. 8.

In the absence of Supreme Court guidance, provincial superior courts have been left to address this issue independently, with little consensus emerging. In Ontario and Saskatchewan, the case law remains inconsistent. In British Columbia, the superior courts have held that a failure to submit a follow-up Report for the extracted data violates s. 489.1 of the *Criminal Code* and thus violates s. 8 of the *Charter*; however, Alberta courts have reached the opposite conclusion. In jurisdictions such as Manitoba, where no case law currently exists on this issue, the question becomes which line of authority should be followed.[69]

A. Ontario

In Ontario, although the courts have been divided on this issue, the majority of decisions, including the most recent, have held that the seizure of data must be reported to a justice.

---

[69] The following list of cases is not exhaustive. They are representative of the current state of the law in their respective jurisdictions. The author was unable to find any Manitoba case law dealing with this specific issue.

1. R v Robinson[70]: A second Report is not required

In *Robinson*, the applicant sought to exclude the data extracted from his seized phone on multiple grounds, including that a second Report to a Justice had not been submitted after the data was seized. The trial judge rejected the applicant's argument that the failure to provide a second report constituted a breach of their *Charter* rights. The judge held that the police had already filed a report for the phone – the "thing" lawfully seized. That phone was seized precisely for the purposes of acquiring data which might prove to be of evidentiary value.[71]

As previously analogized in *Nurse*, the judge likened this process to seizing clothing for the purposes of obtaining DNA or other substances, and concluded that a second report would not be required for information disclosed through the analysis of the clothing.[72] The judge found no reason to justify the separation of the phone from the data contained within it.[73]

From a practical standpoint, the judge in *Robinson* questioned what public policy objectives would be achieved by necessitating a second report. Given that the rationale underlying ss. 489.1 and 490 is to ensure judicial supervision of seized items and their eventual return to the owner, the critical question becomes: what would the justice do with the extracted data?[74]

2. R v Merritt[75]: A second Report is required

The ONSC's decision in *Robinson* diverged significantly from its earlier ruling in *Merritt*. *Merritt* involves the murders of a married couple in 2010 and their son in 2013, allegedly committed by the same perpetrators. Due to ongoing appeals and retrials, the case remains before the courts.[76]

In *Merritt*, the ONSC held that the failure to submit a second Report to a Justice for the data extracted from the accused's computers and USB

---

70 2021 ONSC 2446 [*Robinson*].

71 *Ibid* at para 20.

72 *Ibid* at para 21.

73 *Ibid* at para 22.

74 *Ibid* at para 24.

75 *R v Merritt*, 2017 ONSC 1508 [*Merritt*].

76 Sara Jabakhanji, "Melissa Merritt found not guilty of killing former mother-in-law, faces retrial in ex-husband's murder", *CBC News* (18 March 2024), online: <cbc.ca/news/canada/toronto/melissa-merritt-jury-verdict-1.7147501> [perma.cc/6UCM-V5UD].

keys constituted a breach of s. 8 of the *Charter*. In reaching this decision, the ONSC relied on the Supreme Court's decision in *Vu*, which established that the privacy interest in the data contained on a device is subject to a distinct level of privacy protection, separate from the seizure of the device itself.[77]

3. R v Dacosta & Jeffrey[78]: A second Report is required

In *Dacosta & Jeffrey*, three cell phones were seized from the accused's vehicle incident to their arrest. An initial Report to a Justice was filed. The police later obtained warrants to search the devices; however, no subsequent report was made to the justice describing the results of the search. The accused raised a *Charter* challenge on that basis. The Crown took the position that there was no requirement for a report on the metadata analysis to be submitted to a justice.[79]

The ONSC considered s. 489.1 of the *Criminal Code* and recognized that the extraction of data from an already seized item was not contemplated when the section was enacted, while also being mindful of its earlier decision in *Robinson*. Nevertheless, the court relied on a strict textual interpretation of s. 489.1 to conclude that a second Report to a Justice was required, and that the failure to do so violated the accused's s. 8 *Charter* rights.[80]

4. R v Williams[81]: A second Report is required

In *Williams*, the ONSC was once again tasked with addressing this issue. The court cited the conflicting judgments in *Robinson* and *Dacosta & Jeffrey*, acknowledging the ongoing divide in the case law. It ultimately concluded that the failure by the police to make an independent return for the extracted data from the digital devices constituted a "*meaningful* violation of section 8 [emphasis added]."[82] This determination was based on the finding

---

77 *Merritt*, *supra* note 75 at paras 244-245.

78 2021 ONSC 6016 [*Dacosta & Jeffrey*].

79 *Ibid* at para 41.

80 *Ibid* at paras 42–49.

81 2023 ONSC 4577 [*Williams*].

82 *Ibid* at paras 174-177.

that "[t]he phone and the data each have value both as evidence and as property…"[83]

Notably, the ONSC in *Williams* also found that yet another Report to a Justice should have been submitted when the investigating officer moved one of the devices from the Divisional Property room to the vault at the Technological Crimes Unit, where the data extraction took place.[84] In other words, the transfer of a device lawfully in police custody from one facility to another necessitated further judicial oversight. Respectfully, this finding improperly places form over substance in interpreting s. 489.1, and risks rendering the overall statutory scheme a "meaningless exercise in paperwork."[85]

B. Saskatchewan

Saskatchewan courts are also divided on whether a second Report to a Justice is required for seized data, although recent decisions have concluded that it is not.

1. R v Dick[86]: A second Report is not required

In *Dick*, the Saskatchewan Court of King's Bench (SKKB) held that the preparation of a report by an officer or forensic analyst following a search of an electronic device does not amount to a new or separate "seizure." Echoing the reasoning in *Robinson*, the court emphasized that the device itself is the "thing" seized, while the data retrieved is the product of the search. On this basis, preparing a report does not trigger a second reporting obligation under s. 489.1. The court also questioned the practical purpose of requiring a Report to Justice for data, observing:[87]

> In the case of child pornography data, the police would never return that data to the person lawfully entitled to possess the electronic device. Even if the data is itself not unlawful to possess, there is no evidence before me that when police 'extract' data that they remove it entirely from the device.[88]

---

83 *Ibid* at para 176.

84 *Ibid* at para 173. However, despite the court's finding of a violation of s. 489.1, it was characterized as a "technical breach" which did not violate s. 8 of the *Charter*.

85 *R v Canary*, 2018 ONCA 304 at para 45 [*Canary*].

86 2024 SKKB 155 [*Dick*].

87 *Ibid* at para 68.

88 *Ibid* at para 70.

Accordingly, the court concluded that no *Charter* violation had occurred.

2. R v Herman[89]: A second Report is required

However, in *Herman*, the SKKB held that a failure to report seized data to a justice constituted a breach of s. 8, though it did not rise to the level of necessitating the exclusion of evidence. The court stated, "[i]t defies logic and common sense to think that the evidentiary value of the phones was in the plastic or their other components."[90] Despite this, the court went on to say that the "[r]etention of the [data] seized would *no doubt* have been authorized by a Justice… had the Report to Justice been filed [emphasis added]."[91]

The finding that a justice would have "no doubt" authorized the seizure of the data goes to the heart of the practicality issue. The device had already been lawfully seized and reported to a justice in accordance with s. 489.1, and the police had already sought judicial authorization to search the contents of the device. Thus, there was no absence of judicial oversight at the time the data was extracted. The ultimate legality of the initial seizure of the device, and whether the warrant to search the device was both substantively and technically valid, can be challenged at trial. Absent an identifiable policy objective, the process of submitting another form becomes redundant.

3. R v Pengelly[92]: A second Report is not required

Pengelly again dealt with an investigation into the possession of CSAEM. Officers executed a search warrant at a residence and seized electronic devices pursuant to s. 487 of the *Criminal Code*. Officers also seized additional electronic devices from inside the residence that were not authorized by the warrant, as permitted under s. 489. When the accused was later arrested at a separate location, he was in possession of additional electronic storage devices, which officers seized incident to his arrest. Investigators filed forms for all the physical devices that were seized;

---

89 2023 SKKB 250 [*Herman*].

90 *Ibid* at para 132.

91 *Ibid* at para 133.

92 2024 SKKB 192 [*Pengelly*].

however, none of the forms mentioned the data found on any of the devices.[93]

The SKKB considered the conflicting decisions from *Dick* and *Herman* and ultimately decided that s. 489.1 does not require the police to file a second Report to a Justice for data. Agreeing with the analysis in *Dick*, the court stated:

> The data extracted from a seized electronic device is the product of a search, not a seized "thing" that can be brought before a justice in compliance with s. 489.1(1)(b) of the *Criminal Code*. This does not mean that the owner of the extracted data does not have an enduring, constitutionally protected, privacy interest in the data; it simply means that the s. 490 statutory regime governing the return, continuing detention, and disposal of the seized property does not apply to that data.[94]

C. British Columbia

The courts in British Columbia (BC) have held that a failure by police to submit a second Report to a Justice after data has been "seized" from a device constitutes a *Charter* breach. This authority arises from *R v Bottomley*,[95] which relied on an earlier decision of the BC Court of Appeal (BCCA) in *Craig*.[96]

1. R v Craig: The seizure of data from a neutral third party necessitates reporting to the judiciary

In *Craig*, the police conducted an investigation into online luring. The accused used a third-party server (Nexopia) to exchange messages with a minor for the purposes of meeting and having sexual intercourse. The police obtained a search warrant by telecommunications, pursuant to s. 487.1 of the *Criminal Code*,[97] to access the data stored on Nexopia servers – specifically, the messages exchanged between the accused and the victim.[98] After these messages were "seized" from Nexopia's server, the investigating officer did not file a Report to a Justice, an omission the accused alleged constituted a violation of his s. 8 *Charter* rights.

---

93 *Ibid* at paras 36-42.

94 *Ibid* at para 88.

95 2022 BCSC 2192 [*Bottomley*].

96 *Craig, supra* note 31.

97 *Ibid* at para 157.

98 *Ibid* at paras 3, 4, 13.

The BCCA agreed with the accused. In reviewing various jurisprudence on the issue, the BCCA referenced the Supreme Court's decision in *R v Colarusso*, which described the "continuing nature" of a seizure as follows:

> [I]t must be understood that the protection against unreasonable seizure is not addressed to the mere fact of taking... Protection aimed solely at the physical taking would undoubtedly protect things, but would play a limited role in protecting the privacy of the individual which is what s. 8 is aimed at... The matter seized thus remains under the protective mantle of s. 8 so long as the seizure continues [emphasis in *Craig*].[99]

Ultimately, the BCCA found that the accused's s. 8 rights were violated because of the failure to submit a Form 5.2 for the messages "seized" from the third party.

An important question was not addressed in the *Craig* decision. The messages that were "seized" were not taken from the accused's device or from the device with whom the accused was messaging. Instead, they were "seized" from a third-party website, Nexopia. It is unclear from the written decision why the police chose to seize the messages using a search warrant (or, tele-warrant) instead of requesting Nexopia to produce the messages through a production order.[100] Production orders are the typical method for police to obtain information from neutral third parties, and unlike search warrants, they are not explicitly subject to the s. 489.1 reporting regime.

Whether or not the seizure of data from a neutral third-party engages s. 489.1, under the phrasing "or otherwise in the execution of duties under this or any other Act of Parliament," is beyond the scope of this paper. However, it suffices to say that even if the claimant has a reasonable expectation of privacy in the messages, those privacy interests have already been balanced by the issuing judge or justice. It would be highly unlikely that, even if a Form 5.2 were submitted, a justice would, in any circumstance, order the messages to be "returned" to either the accused or the third-party, assuming such a "return" were even possible.

2. R v Bottomley: The BCSC relies on the Craig decision in finding that a second Report to a Justice for data is required

In *Bottomley*, the police were investigating a homicide and lawfully seized several devices belonging to one of the accused. The police filed the

---

99 *R v Colarusso*, [1994] 1 SCR 20 at para 91, 1994 CanLII 134 [*Colarusso*].

100 *Criminal Code*, *supra* note 3, ss. 487.014, 487.015.

necessary Form 5.2s and obtained judicial authorizations to search the contents of each device. However, no subsequent Form 5.2s were submitted with respect to the data extracted from those devices.[101]

In its decision, the BCSC relied heavily on the BCCA's ruling in *Craig*, stating:

> I agree with the applicants that this binding direction from our Court of Appeal is dispositive of the issue of whether data are a thing seized and thus subject to the reporting requirements of s. 489.1(1) of the Code. In my view, the court must have accepted that extracted data are subject to the Code's reporting requirements in concluding that the police's failure to file a report to justice of the data seized from the social media server constituted a breach of s. 8 of the Charter.[102]

The BCSC determined that the extraction of data from the seized phones constituted a "seizure," reasoning that the applicants "clearly had ongoing privacy interests in the data."[103] In reaching this conclusion, the BCSC gave weight to the SCC's decisions in *Vu* and *Reeves*.[104]

The BCSC then examined aspects of the "totality of the circumstances" test. This test was developed through s. 8 *Charter* jurisprudence to determine whether a reasonable expectation of privacy exists in a given situation.[105] The right to challenge the legality of a search depends on whether the accused had a reasonable expectation of privacy and, if so, whether the search by police was conducted reasonably.[106]

The BCSC relied on *Reeves*, where the Supreme Court characterized the "subject matter of the alleged seizure" as being "what the police were really after."[107] The BCSC found it evident that when searching an electronic

---

101 *Bottomley, supra* note 95 at paras 7, 9.

102 *Ibid* at para 53.

103 *Ibid* at para 47.

104 *Ibid* at paras 45-47.

105 The "totality of the circumstances test" was developed in *R v Edwards*, 1996 CanLII 255 (SCC) [*Edwards*], and further refined in *R v Tessling*, 2004 SCC 67 [*Tessling*]. The test asks four main questions, which need to be tailored to the circumstances of a given case: (1) What was the subject matter of the search?; (2) Does the claimant have a *direct interest* in the subject matter?; (3) Does the claimant have a *subjective* expectation of privacy in the subject matter?; and (4) If so, was the subjective expectation of privacy *objectively* reasonable?

106 *Edwards, supra* note 105 at para 45.

107 *Reeves, supra* note 44 at para 29. In *Reeves*, police seized, without a warrant, a computer belonging to the claimant. Police then obtained a warrant to search the computer,

device, "police are typically interested in the data and information that it contained, not its physical characteristics." Consequently, the Court concluded that the extraction of data constituted a "seizure," given the claimants' ongoing privacy interest in the data.[108]

The issue with the BCSC's analysis in this regard is that it fails to acknowledge that the claimants' inherent privacy interests in electronic devices were already properly considered and balanced by the judge (or justice) who issued the search warrant. In applying for a warrant, police must outline their grounds and explain exactly what they intend to do with the device – namely, to search its contents for evidence relating to a specific offence, as opposed to simply dusting it for fingerprints. Their finding runs directly contrary to the ONSC's decision in *Robinson*, which, as discussed earlier, found that there was no good reason to separate the seizure of the device itself from the data contained therein.

Another issue with the BCSC's determination in *Bottomley* is that it does not address the practicality and public policy issues raised in *Robinson*. If the underlying rationale of ss. 489.1 and 490 is to ensure judicial supervision of items seized by police, what is a justice to do with seized data? The courts would not return CSAEM to the claimant, and given that the extraction process typically does not permanently remove the data from the device itself, what purpose does filing a second Report to a Justice solely for the extracted data serve?

D. Alberta

Recently, Alberta courts have reached the opposite conclusion to their counterparts in BC, finding that no second Report to a Justice for seized data is required.

---

where they located child sexual abuse material. The SCC determined that the subject matter of the search was the computer, and ultimately the data it contained about Reeves' usage, and that police were not after the physical device itself (to collect fingerprints, for example). The SCC ruled that even though police had later obtained a warrant to search the computer, the initial warrantless seizure of the computer constituted a s.8 *Charter* violation, justifying exclusion of the evidence.

108 *Bottomley, supra* note 95 at para 47.

1. R v Simmons[109]: A second Report for seized data is not required, unless it is explicitly demanded by the justice issuing the warrant

Simmons presents an interesting fact scenario. In this case, the police obtained a series of warrants to search the accused's mobile phone as part of a CSAEM and child luring investigation. The police filed an initial Report to a Justice following the seizure of the phone itself,[110] but did not submit any further Reports to a Justice after extracting data pursuant to subsequent warrants.[111] This occurred despite the fact that the warrants to search the device itself contained explicit instructions from the issuing justice directing the police:

> [T]o enter into the said place [the police officer's locker], and to search for the said 'thing' [the cellphone which would be examined for the specified data], and as soon as practicable, *bring them before me or some other Judge or Justice or make a report in respect thereof in accordance with section 489.1 of the Criminal Code* [emphasis added]...[112]

The Alberta Court of King's Bench canvassed the conflicting judgments from BC (*Bottomley*) and Ontario (*Robinson*) and ultimately held that there was no requirement to submit a report concerning the information extracted from a cellphone.[113] However, because the warrants explicitly required that such a report be made, the failure to comply constituted a breach of the warrant's terms and, to that extent, violated s. 489.1 and s. 8 of the *Charter*.[114]

CONCLUSION ON WHETHER EXTRACTED DATA SHOULD BE REPORTED TO A JUSTICE

Parliament's intention in enacting ss. 489.1 and 490 was to establish a regulatory framework for things seized and detained by police. Section 490 outlines the process for the lawful owner of a seized thing to apply for its return. Notwithstanding the fact that Parliament could not have contemplated the seizure of data when these provisions were enacted, the

---

109 2024 ABKB 397 [*Simmons*].

110 *Ibid* at para 118.

111 *Ibid* at para 167.

112 *Ibid* at paras 162, 164, 166.

113 *Ibid* at para 245.

114 *Ibid* at para 217.

question remains: what policy or legal objective would be served in filing a Report to a Justice regarding data? Neither the police nor the courts would ever return CSAEM to the person lawfully entitled to possess the electronic device on which it was stored. Indeed, an accused is not entitled to the return of things seized by police where the trial judge, or a judge to whom an application for restoration is made, is satisfied that the things constitute the fruits of illegal activity.[115]

On a strict interpretation of the text of s. 489.1, it is unclear whether the extraction of data from a device constitutes a "seizure" at all. The data is not permanently removed from the device, and in most cases, the device itself remains undamaged. The mere fact that an officer prepares a report based on the "search" of the data on the device does not mean that the data has been "seized."

Vu and *Reeves* should not necessarily be treated as precedents for whether the subsequent collection of data constitutes a "seizure." While these cases are important in recognizing electronic devices as distinct "places" that warrant higher levels of privacy protection, neither case explicitly characterizes the collection of data as an additional "seizure." Furthermore, the Supreme Court in *Reeves* emphasized that the "subject matter of the search" was not just the physical device itself, but also the informational data it contained – the computer was detained precisely for its contents.[116]

Therefore, when a seized device is included in the initial Form 5.2, the grounds for its seizure and continued detention are already presented to a justice. This weighs against the necessity of a subsequent Form 5.2. Likewise, the prior judicial authorization required to search the device would have outlined both the reasons for the search and the specific information being sought. In other words, the judiciary has already properly considered and balanced the privacy interests in the data.

Does a failure by the Police to submit a Report to a Justice "as soon as practicable" amount to a Charter

115 *R v Aimonetti*, [1981] 3 WWR 42, 5 WCB 448 (Man CA).

116 *Reeves, supra* note 44 at para 30.

BREACH IN ALL CIRCUMSTANCES? IF SO, WHAT IS THE APPROPRIATE REMEDY?

While this paper maintains that a second Report to a Justice should not be required for extracted data, it is important to consider the alternative perspective. If the author's conclusion is incorrect, and the British Columbia courts are correct in holding that a failure to report constitutes a breach of s. 8, the inquiry then shifts to whether exclusion of the evidence is the appropriate remedy. To date, Canadian courts have rarely treated such breaches as warranting exclusion. For example, in *Butters*, although Justice Paciocco found that the police's failure to submit a Form 5.2 for the seized hard drive constituted a serious *Charter* breach, he nevertheless admitted the digital evidence.[117]

Although the Supreme Court has not yet addressed whether non-compliance with the requirements of ss. 489.1 and 490 of the *Criminal Code* results in a breach of s. 8 of the *Charter*,[118] two provincial appellate courts have answered this question affirmatively.[119] These courts have also determined that the admissibility of the impugned evidence should be assessed under s. 24(2) of the *Charter*, using the *Grant*[120] analysis. The following analysis will proceed based on this framework.

The *Grant* analysis is undertaken when evidence has been obtained by a state agent in a manner that infringes on a *Charter* right of the claimant. In such cases, the evidence may be excluded if its admission would bring the administration of justice into disrepute. In certain circumstances, the admissibility of the evidence can also be impacted where the *Charter* breach occurred after the discovery of the evidence.[121] Furthermore, courts have characterized seizures as continuous in nature and have held that so long as

---

117 *Ibid* at 82-85.

118 *R v Paterson*, 2017 SCC 15 at para 58.

119 See *Craig, supra* note 31; and *R v Garcia-Machado*, 2015 ONCA 569 [*Garcia-Machado*].

120 *R v Grant*, 2009 SCC 32 [*Grant*] provides the present framework for determining whether evidence obtained in violation of constitutional rights should be excluded under s. 24(2) of the *Charter*. Because this framework is very often cited and applied in judicial decisions, only a basic overview will be provided in this paper.

121 *R v Pino*, 2016 ONCA 389.

a matter remains seized, it remains under the protection of s. 8 of the *Charter*.[122]

The Grant analysis requires the trier of law to determine whether the admission of the evidence would bring the administration of justice into disrepute. This assessment requires both a long-term and prospective focus, having regard to the societal interest.[123] The court must consider: (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.[124]

As the following cases demonstrate, the failure to submit a Report to a Justice "as soon as practicable" will typically amount to a *Charter* breach. However, in the absence of egregious, intentional or systemic non-compliance, such a failure will rarely justify the exclusion of evidence. Furthermore, the courts have also drawn a distinction between not filing a report at all and not filing a report as soon as practicable.[125]

A. *R v Garcia-Machado*[126]: Evidence admitted on appeal

In *Garcia-Machado*, the accused was charged with impaired driving causing bodily harm. The investigating officer obtained a search warrant to seize hospital records and a vial of blood taken from the accused for medical purposes. However, the officer did not file a Report to a Justice until fifteen months after the seizure and testified that he was unaware that s. 489.1(1) required him to report "as soon as practicable." The trial judge found that the officer's failure to file a timely report violated the accused's s. 8 *Charter* rights and, as a result, excluded the evidence under s. 24(2) and acquitted the accused.

On appeal, the ONCA agreed that the accused's s. 8 rights had been violated but found that the trial judge failed to consider several relevant factors in their s. 24(2) analysis as outlined in *Grant*[127]:

---

122 *Colarusso*, *supra* note 99 at para 91.

123 *Grant*, *supra* note 120 at paras 69, 70.

124 *Ibid* at para 71.

125 See, e.g. *Backhouse*, *supra* note 13.

126 *Garcia-Machado*, *supra* note 120.

127 *Grant*, *supra* note 121.

- The trial judge did not consider that the initial search was authorized by warrant;[128]
- The trial judge failed to consider any factors that created a diminished reasonable expectation of privacy in the records;[129]
- The trial judge similarly failed to consider that the applicant had a minimal residual privacy interest in the hospital records at the time that the reporting period lapsed;[130]
- The trial judge did not consider that the property seized was that specifically authorized by the warrant and that the property was used for the precise purpose for which it was obtained;[131] and
- In cases where the officer had not submitted the report "as soon as practicable," it is "a case of delayed compliance, not of complete non-compliance."[132]

The ONCA in *Garcia-Machado* conducted a fresh *Grant* analysis and concluded that the violation was minor or technical, with no real impact on the accused's *Charter*-protected interests. As a result, the ONCA did not exclude the evidence, overturned the acquittal and ordered a new trial.

The factors outlined by the ONCA in *Garcia-Machado* are directly applicable to the reporting of data "seized" from a device, and weigh heavily against the exclusion of such evidence in the event of delayed or even complete non-disclosure.

B. *R v Canary*[133]: "As soon as practicable" is inherently flexible

The ONCA revisited the leeway provided by the phrasing "as soon as practicable" in s. 489.1 in *Canary*. In this case, police seized a controlled substance from the applicant but did not submit a Report to a Justice for

---

128 *Garcia-Machado, supra* note 120 at para 60.

129 In *Cole, supra* note 54 at para 92, the SCC held that the trial judge, in assessing the nature of the breach, must consider the applicant's *diminished* reasonable expectation of privacy in a work-related computer. Applied to a Report to a Justice, the applicant would have a similarly *diminished* reasonable expectation of privacy in information that was already lawfully possessed by the police.

130 *Garcia-Machado, supra* note 120 at para 61.

131 *Ibid* at para 62.

132 *Ibid* at para 65.

133 *Canary, supra* note 85.

31 days, which the applicant argued constituted a *Charter* breach. Although the ONCA declined to decide whether the 31-day delay amounted to a breach in this case due to the absence of specific facts, the court stated that:

> "There is an inherent flexibility built into the assessment of whether police acted 'as soon as is practicable'. Determining whether this requirement has been met is a necessarily fact-specific inquiry and one that should only be answered after a careful review of all the evidence, including any explanations for why the report was filed when it was."[134]

At the same time, the ONCA underscored the importance of judicial oversight of seized property, cautioning that:

> Section 489.1 should not be conceptualized as a *meaningless exercise in paperwork*. Filing the initial report... is the act that places the property within the purview of judicial oversight. It provides a measure of police accountability when dealing with property seized pursuant to an exercise of police powers [emphasis added].[135]

However, some courts have taken a more "hard-line" approach, finding that a failure by police to comply with the statutory reporting requirements can render an otherwise lawful search unlawful.[136] Whether the evidence should be excluded under s. 24(2) of the *Charter* would depend on whether its admission would bring the administration of justice into disrepute.[137]

C. *R v Neill*[138]: Seven days is not "as soon as practicable" and constitutes a Charter breach

In *Neill*, the police seized a Blackberry device from the accused but did not charge him at the time. Police filed a Report to a Justice for the device seven days later.[139] The officer who seized the device testified that he was occupied with other investigations, and his work shifts did not allow him to file the report immediately.[140] The judge found the seven-day delay in filing

---

134 *Ibid* at para 47.

135 *Ibid* at para 45.

136 See *R v Guiller*, 1985 CarswellOnt 1731, [1985] OJ No 2442.

137 Although *Guiller* was decided prior to *Grant*, the evidence was still excluded.

138 2018 ONSC 5323 [*Neill*].

139 *Ibid* at paras 11, 14.

140 *Ibid* at para 84.

the report to be unreasonable, stating that it was not done "as soon as practicable," and thus constituted a violation of the accused's s. 8 rights.[141]

This finding in *Neill* appears to be the most unforgiving interpretation of s. 489.1 requirements. Even the *1986 LRCC Report*, upon which the present statutory scheme is based, recommended the inclusion of the phrase "as soon as practicable" to take into account the operational realities of police work.[142] Despite determining that the accused's s. 8 rights had been violated, the court in *Neill* nevertheless conducted a *Grant* s. 24(2) analysis and concluded that the evidence should not be excluded.

A similar approach was taken in *Craig*, where the BCCA found that the police's failure to file a Report to a Justice for messages obtained via a telewarrant from a third-party messaging provider amounted to a *Charter* breach. In its *Grant* s. 24(2) analysis, the court emphasized that "the failure to file a Form 5.2 did not affect [the claimant's] rights at all."[143] Because the police conduct was neither egregious nor intentional, and given the limited impact on the accused's protected interests along with the considerable value of the evidence, the evidence was admitted.[144]

The ABCA has supported the view that non-compliance has a negligible impact on a claimant's rights. In specific cases, the ABCA has referred to the requirements set out in section 489.1 as "a routine administrative order," particularly in instances where "there is no reason to believe that a justice would not [grant]" permission to detain the item.[145]

While police non-compliance with the requirements of s. 489.1 generally does not result in the automatic exclusion of evidence, courts have acknowledged that exclusion may be warranted in cases where law enforcement conduct is particularly egregious, intentional, or systematic. In such instances, courts retain the discretion to exclude the evidence, regardless of the seriousness of the offence or the probative value of the evidence itself. The recent BCCA decision in *R v Gill* provides a good example.[146] In *Gill*, police seized several devices from the accused's residence pursuant to a search warrant as part of a murder investigation. Four days

---

141 *Ibid* at paras 84-88.

142 *1986 LRCC Report*, *supra* note 21 at 12-13.

143 *Craig*, *supra* note 31 at para 193.

144 *Ibid* at paras 196-197.

145 *R v Villaroman*, 2018 ABCA 220 at 25.

146 2024 BCCA 63 [*Gill*].

after the phones were seized, police filed an initial Report to a Justice. However, because Mr. Gill had not yet been charged with any offence related to the murder, s. 490(2) of the *Criminal Code* prohibited the detention of the items for more than three months, unless further application was made for continued detention. The police failed to apply for further detention,[147] and the investigation stalled.

Six and a half years later, police obtained a warrant to search one of the devices and discovered an audio-recording of the shooting, which captured Mr. Gill's voice and the sound of gunshots.[148] The evidence was critical, as it identified the accused as being involved in the shooting. Despite this, the BCCA upheld the BCSC's decision to exclude the evidence on the basis that its admission would bring the administration of justice into disrepute, and the charges were stayed. It reasoned that a wilful or reckless disregard of a *Charter* right falls at the more serious end of the culpability scale.[149]

The police conduct in *Gill* was egregious and demonstrated a systemic disregard for the requirements imposed by s. 489.1. However, it is worth considering whether the same outcome would have arisen in an alternative scenario. For instance, imagine that police had possession of that same audio file for six and a half years prior to bringing charges but had failed to submit a subsequent Form 5.2 for that data.

It is unlikely, in this hypothetical, that such conduct would have justified the exclusion of the audio file. The court would have been incapable of "returning" the audio file to Gill, thereby rendering its "oversight" powers moot. Applying the factors from *Garcia-Machado*, the initial search was authorized by a warrant; the accused's expectation of privacy would have been diminished; and the data seized was specifically authorized by the warrant. All these factors weigh against exclusion under a s. 24(2) analysis.

Contrast this with the actual facts in *Gill*, where the police unlawfully and unjustifiably detained the accused's mobile phone for six and a half years. The courts were unable to exercise their oversight over the detained items pursuant to s. 490 of the *Criminal Code*. Had the accused gone to the courts to have his phone returned to him, there would have been no judicial record, beyond the initial Form 5.2 that was submitted, that would have

147 *Ibid* at paras 25, 31.

148 *Ibid* at para 33.

149 *Ibid* at para 105.

indicated that the police were still in possession of the phone. Most importantly, the accused would have been lawfully entitled to the return of his device.

The failure to file a follow-up Report to a Justice for seized data has, until recently, been characterized as a minor administrative or technical breach not justifying exclusion of the evidence. However, as additional cases make their way through the courts, the judiciary may become less sympathetic to the argument that this omission was not made in bad faith by the police. This is evidenced in a recent ruling by the BC Provincial Court, where it stated:

> It seems that it was not general police practice to file a Form 5.2 for data extracted from an electronic device until quite sometime after the B.C. Court of Appeal's 2016 decision in *Craig*. In 2022 the issue was litigated in the B.C. Supreme Court in [unpublished] and in *Bottomley*. One would think that soon after the decision in [unpublished], in or about March 2022, ". If not, one would certainly expect that soon after the release of the *Bottomley* decision on December 4, 2022 filing a Form 5.2 in such cases would be the norm.[150]

CONCLUSION

This paper has argued that a second Form 5.2 should not be required for extracting data from a lawfully seized device, provided that the initial seizure was reported to a justice under s. 489.1 requirements, and a warrant authorizing the search of the device was subsequently obtained. This conclusion is confined to these circumstances and should not be extended to other contexts where data is seized, such as from a "cloud"[151] server or from third-party devices,[152] where heightened privacy interests may necessitate additional judicial oversight under ss. 489.1 and 490.

Canadian case law on this issue remains fragmented. British Columbia stands alone in holding that failure to comply with s. 489.1 in relation to data extraction violates s. 8 of the *Charter*, while Alberta has reached the opposite conclusion. Saskatchewan and Ontario courts have been inconsistent, while other provinces remain silent. Given that the frequency with which these questions arise in investigations into homicides, CSAEM

---

150 *Further Detention of Things Seized (Re),* 2024 BCPC 79 at para 63.

151 Cloud servers are virtual servers hosted by a third-party provider which can be accessed remotely over the internet.

152 See e.g. *R v Marakah*, 2017 SCC 59.

and organized crime, and the increasing modern dependence on technology, it is imperative for the Supreme Court to provide guidance to resolve these consistencies.

Until such direction is provided, police forces in jurisdictions lacking binding authority, such as Manitoba, should err on the side of caution and assume a second Report to a Justice is required. This approach is adopted by the RCMP, as evidenced in their Operational Manual.[153] Nonetheless, situations will inevitably arise where a second Report to a Justice is not submitted. In such circumstances, the divergent case law can be useful in evaluating whether a *Charter* breach has occurred and in assessing its severity.

[153] *Bottomley*, *supra* note 95 at para 27, citing the RCMP Operational Manual, ch 21.3, s. 1.9.3, which instructs that "Data that is seized as a result of investigation must be reported to a justice as soon as practicable, in accordance with CC, section 489.1. NOTE: A 'seizure' includes making a copy of a document."