ULCC | CHLC

UNIFORM LAW CONFERENCE OF CANADA

WORKING GROUP ON SECTION 487 OF THE CRIMINAL CODE

FINAL REPORT

Presented by
Matthew Asma, Chair

Charlottetown
Prince Edward Island
August 2023

Presented to the Criminal Section

TABLE OF CONTENTS

1. INTRODUCTION 2

2. THE CURRENT PROVISION 3

3. CHALLENGES AND RECOMMENDATIONS 6

3.1 Updating the statutory language 7

(a) Remove "suspected to have been committed" 7

(b) Merge paragraphs 487(1)(a), (b), and (c) 9

(c) Remove references to "building" and "receptacle" 11

(d) Consider providing for the inclusion of terms and conditions 13

3.2 Vehicles within the curtilage of a dwelling 15

3.3 Bodily searches of people at the place to be searched 20

3.4 Entering a place to make observations and measurements 23

3.5 Authority for examination of data within or available to a seized computer 27

3.6 Accessing and copying computer data by remote means 43

3.7 Correcting errors in unexecuted warrants 49

3.8 Warrants authorizing entry at night 50

3.9 Sealing and non-publication provisions 52

4. SUMMARY OF RECOMMENDATIONS 58

APPENDIX: CRIMINAL CODE SECTION 487 AND FORM 5 63

1. INTRODUCTION

[1] At the 2018 annual meeting of the Criminal Section of the ULCC, the following resolution (Can-CBA2018-05) was adopted:

> A working group should be formed to review section 487 of the *Criminal Code* (information for search warrant) and examine how this investigative power should be modernized, taking into account new technologies, the *Canadian Charter of Rights and Freedoms* and relevant national and international developments. At the discretion of the working group, it will report back to the Section with either an interim or final report at the next conference.

As a result, this Working Group was formed. Status reports were presented at subsequent annual meetings. This is the final report of the Working Group, for presentation at the 2023 annual meeting.

[2] The Working Group has interpreted its mandate to relate to a general-purpose criminal law authority for judicial preauthorization of overt (as opposed to covert) search and seizure. Surreptitious search and surveillance tools such as intercepting private communications, covert video surveillance of private spaces or activities, covert entries into private premises, and covert techniques for accessing data, were considered to be beyond the scope of this work. Similarly, production orders (that is, orders to compel a record-holder to produce documents or data to a law enforcement official) were not considered by this Working Group; although production orders are overt in the sense that the record-holder must be served with the order, production orders are often covert in the sense that the person under investigation may have no way of knowing the search has occurred. The Working Group has therefore focused on searches of physical premises, conveyances (vehicles), people, and computers. It may seem that searches involving computers and data are of a different nature than the other types of searches mentioned; however, under the current legislative scheme, section 487 search warrants are the tool most commonly used to authorize computer searches, and the resulting legal issues are among reasons that section 487 is overdue for reform.

[3] Additionally, the Working Group considered certain kinds of post-seizure examinations of seized objects that may require additional judicial authorization, beyond the authority that is implicit in the authorized seizure of the physical object. For example, case law dictates that a person can sometimes maintain a reasonable expectation of privacy in computer data, or in biological information in some circumstances, even after police have lawfully seized the physical object that carries a representation of the data or the biological information. The Working Group therefore considered the creation of a new general-purpose examination warrant that can either be coupled with a search warrant or granted separately.

[4] At the 2022 annual meeting, it was resolved that consideration of sections 489.1 and 490 of the *Criminal Code* should be studied by this Working Group in relation to issues around the treatment of data under those sections (Can-PPSC2022-01). However, at the same annual meeting, the section 490 Working Group was reconstituted. The chair of this Working Group was given the opportunity to read a draft version of the 490 Working Group's report, in May of 2023. The proposals in this report do not appear to be in conflict with the direction taken by the 490 Working Group's draft report.

[5] Members of the Working Group who contributed to this report were: chair: Matthew Asma (Ministry of the Attorney General, Ontario), past chair: Normand Wong (Justice Canada), and members: Karen Audcent (Justice Canada), Greg DelBigio (Canadian Council of Criminal Defence Lawyers), Sandro Giammaria (Justice Canada), Kenyata Hawthorne (Justice Canada), Pauline Lachance (Directeur des poursuites criminelles et pénales, Québec), Anne-Marie Lebel (Justice Canada), Karen Lee (New Brunswick Attorney General, Public Prosecution Services), James Meloche (Public Prosecution Service of Canada), Nadine Nesbitt (Alberta Crown Prosecution Service), Paul Pearson (British Columbia Ministry of the Attorney General), Christopher Samuel (Canadian Bar Association / University of Alberta), Andrew Synyshyn (Criminal Defense Lawyers Association of Manitoba), and Anna Zhang (articled student, Ministry of the Attorney General, Ontario). Past member Randy Schwartz (Ministry of the Attorney General, Ontario) contributed significantly to an early draft of the report.

2. THE CURRENT PROVISION

[6] Section 487 has remained largely unchanged since its introduction in 1892 when Parliament first enacted the *Criminal Code*. The section sets out the procedure and legal standard that must be followed to obtain a judicially preauthorized warrant to search a place and seize things prescribed in the warrant (a "487 warrant").

[7] A 487 warrant is available for, and limited to, authorizing entry into a "building, receptacle or place," to search for and seize "things" that are currently in that building, receptacle or place. The main purpose of the provision is to allow law enforcement to find, seize, and preserve things that "will afford evidence" of an offence.[1] The warrant must clearly identify the place to be entered and searched, and the thing or things to be

[1] The most-used route to issuance of a 487 warrant is paragraph 487(1)(b), which requires reasonable belief on the part of the applicant that seizure of the thing "will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence." The term "will afford evidence" has been interpreted broadly and it is not limited only to finding evidence that proves the alleged offence: *CanadianOxy Chemicals Ltd. v. Canada (A.G.)*, [1999] 1 S.C.R. 743; *R. v. Vice Media Canada Inc.*, 2018 SCC 53 at para. 47.

searched for and seized. One hundred and forty years of judicial interpretation has expanded the scope of the warrant somewhat to adapt to the modern environment (for example, 487 warrants are now routinely used to authorize examination of computer data after the computer is physically seized), but the 487 warrant remains fundamentally an authority that allows agents of the state to invade a person's privacy in relation to a physical space, and to seize tangible things.

[8] Section 487 sets out preconditions that must be met before a judicial official can issue a warrant, including whether there is a reasonable basis for the applicant's belief that an offence has been committed, and whether there is a reasonable basis for believing the search and seizure will afford evidence with respect to the commission of the offence. If the preconditions are met, a justice may issue a warrant authorizing law enforcement to enter and search the place for the things listed in the warrant, seize them, and return with them to a justice or make a report to a justice about the things seized. The warrant also specifies the timeframe during which law enforcement may enter the place and begin to search it; that time is presumed to be during daytime hours unless night execution has been specifically justified and authorized (section 488). While in the place, anyone executing the warranted search is also empowered to seize any additional thing not listed in the warrant, if they reasonably believe that the additional thing was obtained by crime, or used in the commission of a crime, or will afford evidence of a crime (subsection 489(1)).

[9] Previously, the out-of-province execution of a 487 warrant required the endorsement of a judicial officer with jurisdiction in the province where the warrant is to be executed. As of a 2019 amendment, the section now allows for a 487 warrant to be executed at any place in Canada by a peace officer, or public officer named in the warrant, who has the authority to act in that capacity in the place where the warrant is executed (subsection 487(2)).

[10] While criminal activity has evolved and adapted to the benefits of advancing technology, the investigative tools available to police in section 487 have not kept pace. Section 487 and its companion provisions in sections 488 (execution of a warrant), 489 (seizure of things not specified) and 490 (detention of things seized) were designed to allow the state to intrude upon a private place and seize physical property. That paradigm of search and seizure is no longer sufficient for effective criminal investigations in the 21st century.

[11] For example, the 487 warrant is ill-suited to authorizing the search for and seizure of forms of evidence that are primarily intangible, such as data. In 1892, when what is now section 487 was enacted, many of the important "intangibles" of current times – including computer data, digital assets, and genetic profiles derived from biological matter – had not been envisioned as being potentially subject to a search and seizure. Indeed

neither the electronic transistor nor the DNA molecule had yet been discovered. To take the example of computer data: In 1892, any data that might be of interest in a criminal investigation would be represented on a human-readable, tangible medium (typically paper or parchment) that was capable of being physically seized. Although multiple copies might exist, whether through the work of a human scribe or a printing press, each copy would have a unique physical existence and thus could only be in one place at any given time. Seizing the tangible medium almost inevitably deprived the owner of access to the data. In 2023, it is a rare criminal investigation that does not, in some way, involve data stored in an electronic medium. Rather than a physical copy being unique, electronic representations of data can be reproduced, with negligible delay, in perfect fidelity to the original. Multiple exact copies of data may reside on complex networked storage devices whose location or locations are, for practical purposes, both multiple and unascertainable.[2] There may be no single "place" to search, and no single "thing" to seize. Furthermore, seizing one copy does not necessarily deprive someone else of the data. Many common-sense assumptions that must have lain behind the drafting of section 487 and its companion provisions are simply no longer true.

[12] In 1997, section 487 was amended to allow for searches for data contained in or available to a computer system located in the place to be searched. That provision, found in subsection 487(2.1), is drafted in a way that authorizes police to seize something tangible, that is, data "reproduced… in the form of a print-out or other intelligible output" following the search of a computer system. That drafting choice has the virtue of maintaining consistency with the traditional notion of seizing tangible things. However, it does not directly authorize the seizure of purely intangible evidence, and it presents other challenges for law enforcement that are discussed later in this report. In the result, subsection 487(2.1) is not often used.

[13] Since its inception, the common law relating to search warrants has assisted in the search warrant's evolution, and clarified some instances when these warrants can be used (*e.g.*, for fingerprints, blood, gunshot residue, and other trace evidence at a crime

[2] "Cloud" data storage providers may maintain redundant copies of data at different locations, and may spread a particular set of data across different file servers at different locations. The file servers and locations used for a particular set of data may shift from time to time as the system automatically works to balance the loads on individual components of the distributed system; or as equipment is replaced or upgraded; or to achieve other optimization goals that are completely opaque to the human user. See *e.g.*, Walden, Ian, "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (Second Edition)" (May 1, 2021), in Millard, C. (ed.), *Cloud Computing Law* (2nd ed., Oxford U. Press 2021), Available at SSRN: https://ssrn.com/abstract=4227129.

scene[3]). However, other forms of "overt" searches, such as the bodily search of a person, taking photos or measurements of a place, cannot be authorized by section 487. On one view, the search of a vehicle found at the place named in the warrant is not authorized by a warrant to search that place. Other types of warrants (*e.g.* the general warrant in section 487.01) or warrantless search authorities available at common law (*e.g.* search incident to arrest) are sometimes available to fill certain gaps. But those other tools have limits and reliance on them poses challenges. The common law power of search incident to arrest, for example, is only available when police actually arrest the individual, and thus is of no assistance in conducting the investigation before an arrest is made. The general warrant provides for preauthorization of some kinds of searches for which there is no other form of warrant available, but the additional preconditions for issuing a general warrant introduce nuanced legal questions that make them poorly suited for routine investigative use.[4]

3. CHALLENGES AND RECOMMENDATIONS

[14] In its review, the Working Group has identified challenges and made recommendations in nine areas of concern:

1. Updating the statutory language and harmonizing it with other current search and seizure powers in Federal criminal law
2. Clarifying an issue about whether a vehicle found within the curtilage of a dwelling can be searched on the authority of a warrant to search the dwelling
3. Providing authority for bodily searches of persons found at the place to be searched in certain circumstances

---

[3] *E.g.*, *R. v. Plant*, 1991 ABCA 116 at para. 12 (aff'd on other grounds [1993] 3 S.C.R. 281) (fingerprints); *R. v. Thomas*, 2013 ONSC 8032 at paras. 41-46 (blood); *R. v. Kabanga-Muanza*, 2018 ONSC 6514 at paras. 161-172 (fingerprints, DNA, gunshot residue).

[4] It is a precondition for issuing a general warrant that there is "no other provision" in Federal law providing for preauthorization of the specific technique sought to be authorized by the general warrant: section 487.01(1)(c). This is a legal question that can provoke challenging debates among lawyers and judges (*e.g.*, *R. v. Ha*, 2009 ONCA 340; *R. v. Telus Communications Co.*, 2013 SCC 16). It is not desirable that police officers should need to wade into those legal debates in routine cases. Another practical obstacle is that general warrants can only be issued by judges, making them less convenient for police to obtain in jurisdictions where most warrants are issued by justices of the peace.

4. Providing authority for a warrant to enter a place and make observations, including by means of telecommunication
5. Improving the means of authorizing post-seizure examination or analysis of computers and computer data
6. Updating the existing tools for remotely accessing and copying computer data
7. Providing a statutory authority for correcting errors in unexecuted search warrants
8. Clarifying the legal test for search warrants that authorize entry at night
9. Clarifying and fixing several issues around existing provisions that deal with sealing and non-publication of search warrants materials

3.1 Updating the statutory language

[15] There are several ways in which the language of section 487 has not kept up with Charter jurisprudence, or contains unnecessarily archaic or redundant language. Generally, the language of the section should be modernized to bring it into harmony with more recently-enacted search and seizure powers in the *Criminal Code* and the search warrant provision in section 11 of the *Controlled Drugs and Substances Act*.

(a) Remove "suspected to have been committed" in the English text

[16] The rarely-used paragraph 487(1)(a) provides, in the English text only, that a warrant may issue to search for and seize "anything on or in respect of which any offence… has been or is suspected to have been committed". A leading textbook on search and seizure notes that warrants under paragraph 487(1)(a) are "rarely used" and, for reasons discussed next, recommends that paragraph 487(1)(a) should not be used.[5]

[17] The language of "suspected to have been committed" has repeatedly contributed to drafting errors by police or the issuing justice, leading to warrants being found invalid (the "*Branton* error"). Moreover, the suspicion standard sits uncomfortably with the legal threshold of "reasonable grounds to believe" that is expressed in the text of subsection 487(1), and that was held to coincide with the default constitutional standard for pre-authorized searches that comply with section 8 of the *Charter*.[6]

---

[5] Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at pp. 93-94.

[6] *Hunter et al. v Southam Inc.*, [1984] 2 S.C.R. 145 at p. 168: "In cases like the present, reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search,

[18] In the case of *R. v. Branton*,[7] the Ontario Court of Appeal held that a warrant issued under paragraph 487(1)(b), based on reasonable grounds to believe the things to be seized would afford evidence, was facially invalid for purporting to authorize seizure of things in respect of which an offence was "suspect to have been committed." Essentially, the wrong box had been checked on a version of Form 5 (the prescribed form for a 487 warrant), thereby incorporating language from paragraph (1)(a) into a warrant issued under paragraph (1)(b). Subsequent courts encountering similar errors in a 487 warrant have sometimes held that the "suspected to have been committed" language could be severed from the warrant, such that the remaining warrant was valid.[8] Other courts have held that warrants were invalidated by reason of a "*Branton* error."[9]

[19] The language of "suspected to have been committed" also appeared in the original version of the production order power (then section 487.012), enacted in 2004. The provision was re-enacted in slightly different form in 2014 (now section 487.014) and "suspected to have been committed" was removed in the process. At least one court has considered the constitutionality of the since-repealed language, and declared the words "suspected to have been committed" in former section 487.012 to be inoperative for not complying with the *Hunter v. Southam* constitutional standard.[10]

[20] The words "suspected to have been committed" are not present in the search warrant provision in section 11 of the *Controlled Drugs and Substances Act*, nor in section 87 of the *Cannabis Act*.

[21] In a bilingual enactment, the French and English texts are equally authoritative

---

constitutes the minimum standard, consistent with section 8 of the *Charter*, for authorizing search and seizure." Later decisions have held that the lower standard of "reasonable suspicion" may be compliant with section 8 of the *Charter* in contexts where there is a lower expectation of privacy: *R. v. Kang-Brown*, 2008 SCC 18 at para. 59.

[7] *R. v. Branton* (2001), 144 O.A.C. 187 (C.A.) at paras. 35-36.

[8] *R. v. Jacobson*, 2004 CanLII 5912 (Ont. S.C.J.) at paras. 43-57; *R. v. Nurse and Plummer*, 2014 ONSC 1779 at paras. 27-40 (aff'd on other grounds 2019 ONCA 260); *R. v. Nguyen*, 2017 ONSC 1341 at paras. 112-16; *R. v. Owen*, 2017 ONCJ 729 at paras. 125-33

[9] *R. v. N.N.M.*, 2007 CanLII 31570 (Ont. S.C.J.) at paras. 331-35; *R. v Persaud*, 2016 ONSC 8110 at para. 211; *R. v. Kramshoj*, 2017 ONSC 2951; *R. v. Pahle*, 2017 ONSC 6164 at para. 74

[10] *R. v. Grandison*, 2016 BCSC 1712 at paras. 85-96. Also see the dissent in *R. v. Fedossenko*, 2014 ABCA 314, and contrast the majority in *R. v. Fedossenko*, 2014 ABCA 314, and *R. v. Nero*, 2016 ONCA 160 at para. 62.

and their proper interpretation requires identification of their shared meaning when possible.[11] However, in paragraph 487(1)(a), the French version[12] does not use language that signifies a suspicion standard. The French text says "*présumée avoir été commise*". That phrase appears at multiple other locations in the *Criminal Code* where it is the analog of the English phrase "alleged to have been committed." The word "*présumée*" also appears in paragraph 487(1)(b), where it is the analog of "believed". Given that belief and suspicion are different legal standards, it is difficult to interpret a shared meaning from the French and English versions of paragraph 487(1)(a). This is further reason that the text needs to be revised by removing "suspected" from the English version.

[22] In summary, the words "suspected to have been committed" have repeatedly been a source of drafting errors that can lead to warrants being found invalid. And quite apart from drafting errors, the phrase may itself be constitutionally vulnerable in a general-purpose search provision. Moreover, the lower legal standard denoted by the word "suspected" is not reflected in the French text, which is better interpreted as requiring that the offence is "believed" to have been committed. The reference to suspected commission of an offence should be removed from the English version of the provision.

Recommendation 1.1:

The Working Group recommends that the words "suspected to have been committed" be removed from section 487 of the *Criminal Code*.

(b) Merge paragraphs 487(1)(a), (b), and (c)

[23] After removing the words "suspected to have been committed", there is not much left of paragraph 487(1)(a). Without the constitutionally dubious suspicion standard, it appears that anything which could be seized pursuant to paragraph 487(1)(a) can alternatively be seized pursuant to paragraph 487(1)(b) [things that afford evidence of an offence] or paragraph 487(1)(c.1) [offence-related property].[13] And as already noted, paragraph 487(1)(a) is rarely used in contemporary practice.

[24] The Working Group discussed whether subsection 487(1) gains anything by being further subdivided into its four existing paragraphs, (a), (b), (c), and (c.1). Consensus developed that functionally, there are really only two categories that need to be captured

---

[11] *R. v. Daoust*, 2004 SCC 6 at paras. 2, 26.

[12] See the Appendix to this report for the bilingual text of the section.

[13] Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at pp. 93-94.

by the legislation, not four. First, paragraphs (a), (b), and (c) represent investigative purposes that are about gathering evidence in a broad sense. In a modernized section 487, these should be merged into a single clause that is centred around the concept of searching for and seizing things that "will afford evidence" of the offence under investigation.[14]

[25] Second, paragraph 487(1)(c.1) provides for warrants to search for and seize "offence-related property". Offence-related property is defined in section 2 as:

> any property, within or outside Canada,
> (a) by means or in respect of which an indictable offence under this Act or the *Corruption of Foreign Public Officials Act* is committed,
> (b) that is used in any manner in connection with the commission of such an offence, or
> (c) that is intended to be used for committing such an offence.

[26] The *Criminal Code* provides a comprehensive scheme for the restraint, management, and forfeiture of offence-related property in sections 490.1 through 490.9. The ability to issue a search warrant for seizure of offence-related property is an important complement to that scheme, and the *Criminal Code* should maintain an authority to grant warrants to search for and seize offence-related property. Paragraph 487(1)(c.1) should therefore be maintained as part of the search warrant scheme, although as a matter of drafting it may make sense to move it to a different subsection of the provision given that a seizure of things that "will afford evidence" is conceptually different from a seizure of things that are "offence-related property." However the provision is reorganized, it should remain possible for police to get a single warrant that authorizes searching both for things that will afford evidence and for things that are offence-related property.

Recommendation 1.2:

The Working Group recommends that paragraph 487(1)(a), (b), and (c) of the *Criminal Code* be combined into a single subsection that is focused on seizing things that will afford evidence of an offence, based on the legal standard of reasonable belief and without reference to suspected offences. The function of current paragraph 487(1)(c.1), that is, providing authority for seizure of offence-related property, should be maintained.

[14] The phrase "will afford evidence" has been authoritatively interpreted to have a very broad meaning. It is not limited to finding evidence that proves the alleged offence: *CanadianOxy Chemicals Ltd. v. Canada (A.G.)*, [1999] 1 S.C.R. 743; *R. v. Vice Media Canada Inc.*, 2018 SCC 53 at para. 47.

(c) Remove references to "building" and "receptacle"

[27] Section 487 provides for warrants to enter and search buildings, receptacles or places. The phrase "building, receptacle or place" appears in the original 1892 *Criminal Code* and remains, unchanged, today. Regardless of whether there was ever a reason to enumerate buildings and receptacles separately from places, there is an argument that from today's perspective, the terms "building" and "receptacle" are redundant. That is, anything that is a "building" or "receptacle" is also a "place."

[28] Appellate courts have implicitly treated "place" as a compendious term that includes buildings and receptacles, in the context of search warrants.[15] Other search authorities in Federal legislation refer to places without also referring to buildings and receptacles. On this view, the words "building" and "receptacle" are obsolete.

[29] However, the Working Group's discussions lead us to a different conclusion. It is undoubtedly true that any "building" is also a "place". It is less clear that any "receptacle" is necessarily a "place" — particularly if the receptacle is something mobile, like a portable container, or a vehicle. The Working Group recommends that the language of section 487 should be simplified, with no loss of function, by changing "building, receptacle or place" throughout subsection 487(1) to simply "place." Similarly, in subsections (2.1) and (2.2), "building or place" could be changed to just "place". However, to ensure that a broad meaning of "place" in section 487 is understood by users of the statute, the Working Group recommends a new definitional clause that states:

> In this Part, "place" includes a building, receptacle, or conveyance as defined in section 320.11.

The new reference to conveyances[16] is for reasons that are discussed in Part 3.2 of this report. (In brief, this will help resolve an ambiguity about authority for searching vehicles adjacent to dwellings.)

[30] For comparison, section 487.01 of the *Criminal Code*, the general warrant provision, provides for the issuance of a warrant to use a device or perform a technique or

---

[15] *E.g.*, *R. v. Vu*, 2013 SCC 60 — the statutory words "building, receptacle or place" are quoted only in a single paragraph (para. 44), whereas "place" standing alone is otherwise used through the decision. Similarly, *R. v. Jones*, 2011 ONCA 632 at paras. 47-49 — where a dwelling (building), and cabinets, drawers and vaults (receptacles) and computers were all discussed as potential "places" to be searched, without use of the redundant language of buildings and receptacles.

[16] *Criminal Code* section 320.11: "conveyance" means a motor vehicle, a vessel, an aircraft or railway equipment.

procedure that is not otherwise capable of being authorized under Federal law. Subsection 487.01(5.1) imposes a requirement for after-the-fact notice when a "place" is searched covertly by way of a general warrant. It is evident that "place" is meant broadly, and it certainly applies to covert entries into buildings and other private physical spaces, despite the enactment making no mention of buildings or receptacles.

[31] Another useful comparison is the former section 487.1 of the *Criminal Code*, the telewarrant provision (repealed and replaced in January 2023), which provided for the issuance of a telewarrant when it was impracticable to obtain a 487 warrant. Former section 487.1 spoke of "the place or premises to be searched". Telewarrants could and did issue for places that are buildings, and for places that are receptacles, despite the text of the provision not specifically referring to buildings or receptacles.

[32] Further, subsection 489(2) of the *Criminal Code* provides for seizure of things in plain view that an officer believes will afford evidence of an offence when the officer "is lawfully present in a place." There is no mention of buildings or receptacles in the provision, but nobody would argue that subsection 489(2) is unavailable if the officer is located in a building; a building is plainly within the meaning of "place" in subsection 489(2).

[33] Outside of the *Criminal Code*, section 11 of the *Controlled Drugs and Substances Act* and section 87 of the *Cannabis Act* both refer simply to searching "a place." There is no discernable disadvantage to police in obtaining warrants to search buildings and receptacles when operating under those statutes.

[34] It is also noteworthy that section 98 of the *Criminal Code*, which defines the offence of breaking and entering to steal a firearm, explicitly states that "*place* means any building or structure — or part of one — and any motor vehicle, vessel, aircraft, railway vehicle, container or trailer." Although not directly relevant to the search warrant context, this provides further illustration that Parliament can and does use "place" to encompass a wide range of objects, including buildings, vehicles and containers. In other words, it is not inconsistent with other *Code* provisions if "place" is given a broad meaning.

[35] The Working Group also observed that the term "dwelling-house" appears in Form 1 (the prescribed form for an information to obtain a search warrant), and the term "premises" appears in Form 5 (the prescribed form for a search warrant), although neither term appears in the authorizing section 487. As discussed in Part 3.2 of this report, "dwelling-house" has a confusing and convoluted statutory definition. The Working Group recommends that the wording of the prescribed forms should better adhere to the statutory language in section 487 by removing "premises" and "dwelling-house" from the forms.

Recommendation 1.3:

The Working Group recommends that the terms "building" and "receptacle" be deleted throughout section 487 of the *Criminal Code*, leaving only the word "place." A new definition of "place" should be added, stating that a place includes a building, receptacle, or conveyance. Confusing references in Form 1 and Form 5 to "premises" and "dwelling-houses" should be removed.

(d) Consider providing for the inclusion of terms and conditions

[36] Section 487 currently does not explicitly allow for the inclusion of terms or conditions in a 487 warrant, other than the mandatory requirement to make a report to a justice after seizing things (required by paragraph 487(1)(e)), the requirement to give or affix a copy of a Notice of Execution of Search warrant in Form 5.1 (required by section 487.093 of the *Criminal Code*), and the requirement to state a time for execution (required by Form 5). Given that the issuance a 487 warrant is discretionary, it is undoubtedly open to a justice to impose additional conditions that limit the scope of the authority conferred by the warrant.[17] There is a view that providing an explicit statutory basis for the optional inclusion of other conditions in a 487 warrant would improve consistency with other *Criminal Code* provisions, and would encourage both police and judicial officials to consider whether impacts on privacy rights can be mitigated by prescribing conditions. There is also an opposing view.

[37] Other search provisions in the *Criminal Code* explicitly invite the inclusion of conditions to ensure the search is reasonable. In the general warrant provision, subsection 487.01(3) provides:

> A warrant issued under subsection (1) shall contain such terms and conditions as the judge considers advisable to ensure that any search or seizure authorized by the warrant is reasonable in the circumstances.

In the production order scheme, subsection 487.019(1) provides:

> An order made under any of sections 487.013 to 487.018 may

[17] *Descôteaux v. Mierzwinski*, [1982] 1 S.C.R. 860 at 889: "The justice of the peace, in my view, has the authority, where circumstances warrant, to set out execution procedures in the search warrant…". Also see *Baron v. Canada*, [1993] 1 S.C.R. 416, holding that the discretionary nature of search warrants is a constitutional requirement under the *Charter*.

> contain any conditions that the justice or judge considers appropriate including, in the case of an order made under section 487.014, conditions to protect a privileged communication between a person who is qualified to give legal advice and their client.

The scheme for DNA warrants and DNA orders provides in subsection 487.06(2):

> The warrant, order or authorization shall include any terms and conditions that the provincial court judge or court, as the case may be, considers advisable to ensure that the taking of the samples authorized by the warrant, order or authorization is reasonable in the circumstances.

In contrast, the search warrant provisions in the *Controlled Drugs and Substances Act* (section 11) and in the *Cannabis Act* (section 87) are more like section 487 in that they do not explicitly invite the inclusion of terms and conditions. But like section 487, the optional addition of terms and conditions in those other warrants is undoubtedly allowed as part of the exercise of discretion of the issuing justice.

[38] The Working Group debated arguments both for and against a new provision that explicitly invites inclusion of terms and conditions in a search warrant.

[39] Arguments in favour of providing for this option explicitly in the statute are that:

- Adding a statutory provision explicitly allowing for the inclusion of terms and conditions may remind investigators who apply for search warrants, and justices who decide whether to grant them, to consider whether any optional terms or conditions are necessary to ensure the search or seizure is reasonable.

- Several other modern search provisions in the *Criminal Code* already have explicit provisions to this effect (production orders; general warrants; DNA warrants), and consistency of practice would be enhanced by re-drafting section 487 with the same approach.

[40] Against a change of this nature are these arguments:

- The authority to add terms and conditions when granting a search warrant is already implicit, and the authority is used when it is needed. But adding an explicit provision that invites the justice to consider adding terms and conditions may be interpreted as a new direction from Parliament to change exist-

ing practice, making justices more interventionist and resulting in ill-considered changes being made by the issuing justice without input from investigators. Most concerning, if justices are explicitly directed to consider adding terms and conditions, there is a risk that conditions will be inserted that either have no foundation in the evidence provided in the affidavit, or that stray outside the proper role of the issuing justice.

- Conditions on the manner of execution of a warrant are not always possible to determine appropriately in advance, as is reflected in the Supreme Court of Canada's recognition that the manner of execution of a search should be reviewed after the fact, and not generally prescribed in advance in the warrant.[18]

Recommendation 1.4:

The Working Group recommends that Parliament should consider whether section 487 *Criminal Code* should be amended to explicitly allow that the issuing justice may include terms and conditions that the justice considers appropriate to ensure the warrant is reasonable.

3.2 Vehicles within the curtilage of a dwelling

[41] There are two mutually contradictory lines of authority in the Canadian jurisprudence about whether a motor vehicle that is parked near a dwelling that is authorized by a 487 warrant to be searched can itself be searched under the authority of the warrant. In other words, if police obtain a 487 warrant to search a dwelling, does that warrant also authorize the search of a motor vehicle parked adjacent to the dwelling? The long-running legal uncertainty arising from this question deserves to be settled by legislation.

[42] The controversy relates to the statutory definition of "dwelling-house"[19] in section 2 of the *Criminal Code*:

> "dwelling-house" means the whole or any part of a building or structure that is kept or occupied as a permanent or temporary residence, and includes
>
> > (a) a building within the curtilage of a dwelling-house that is connected to it by a doorway or by a covered and enclosed passage-way, and

[18] *R. v. Cornell*, 2010 SCC 31.

[19] The term "dwelling-house" is not used in section 487 itself, but it appears in Form 1 where the affiant it asked to describe the building, receptacle, or place to be searched.

> (b) a unit that is designed to be mobile and to be used as a permanent or temporary residence and that is being used as such a residence

[43] The statutory definition suggests, but does not explicitly say, that the curtilage is part of the dwelling-house. At common law, curtilage is the area of land attached to and immediately surrounding the dwelling.[20] It is well established that a warranted search of a dwelling can extend to its curtilage, although it is often debated whether the conduct of the search in fact strayed beyond the limits of the curtilage and/or the specific wording of the warrant in issue.[21]

[44] Some courts in Ontario have accepted the proposition that a motor vehicle parked on the driveway of a dwelling may be searched pursuant to a warrant for search of the dwelling, based on the motor vehicle being within the curtilage of the dwelling.[22] The Ontario Court of Appeal wrote, "Certainly if the car had been in the garage of the premises or even on the driveway there would be little doubt that the search warrant would cover a search of the car."[23] However, the same proposition has been rejected in several other courts, including the British Columbia Court of Appeal.[24]

[45] It should be noted that a motor vehicle parked within the dwelling (*e.g.* inside an attached garage or a connected carport) is clearly searchable under a warrant to search the dwelling. This is because any container found within the place to be searched can

---

[20] *R. v. Lauda* (1999), 45 O.R. (3d) 51 (C.A.); *R. v. Le*, 2011 MBCA 83 at paras. 78-80; Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at p. 119.

[21] *R. v. Tesfai*, 1995 CanLII 4153 (N.S.S.C.) (curtilage included a patio, but not a space several feet beyond the patio); *R. v. N.N.M.*, 2007 CanLII 31570 (Ont. S.C.J.) at paras. 367-76 (curtilage did not include detached outbuildings); *R. v. Le*, 2011 MBCA 83 at paras. 96-100 (curtilage included flower beds and contiguous fenced back yard); *R. v. Lindsay*, 2015 ONSC 1369 at para. 184 (curtilage included the fenced backyard); *R. v. Burkoski*, 2017 ONSC 7399 at paras. 24-35 (curtilage did not include the detached shed).

[22] *R. v. Haley* (1986), 27 C.C.C. (3d) 454 (Ont. C.A.); *R. v. Osanyinlusi*, 2006 CanLII 21070 (Ont. S.C.J.) at paras. 54-55, aff'd on other grounds 2008 ONCA 805.

[23] *R. v. Haley* (1986), 27 C.C.C. (3d) 454 (Ont. C.A.) at 465.

[24] *R. v. Brennen*, [2000] O.J. No. 3257 (S.C.J.) at paras. 68-69; *R. v. Do*, 2002 BCSC 1889 at para. 12; *R. v. Vu*, 2004 BCCA 230 at paras. 20-33; *R. v. Vo*, 2011 ABQB 701 at paras. 27-32. The *Haley* decision was also not followed in *R. v. Clarke*, 2012 ONSC 1259 at paras. 68-77, although the Court's reasoning seems to turn on the wording of the specific warrant in issue rather than the general propriety of searching the curtilage of a dwelling.

itself be searched,[25] provided it is capable of containing one of the things that the warrant authorizes police to search for and seize.[26]

[46] It is true that a motor vehicle can be specifically described in the warrant as part of the place to be searched, much like a detached outbuilding can also be specifically listed.[27] Indeed this is clearly the safer drafting practice for police to follow, given the current uncertainty of the jurisprudence on the issue.[28] However, the vehicle-in-curtilage controversy still deserves to be clarified, since police do not always know in advance of executing the warrant that a motor vehicle will be parked at a dwelling.

[47] One solution to clarify the issue would be to provide that a dwelling-house includes its curtilage and any motor vehicle that is located within the curtilage. This would put motor vehicles on the same legal footing as any other container that happens to be situated in the curtilage of the dwelling-house at the time a search warrant is executed.

[48] Another solution would be to provide that although a dwelling-house includes connected buildings (as the definition now provides), a dwelling-house does not include a motor vehicle unless it is located within the dwelling or a connected structure. This would grant a special legal status to motor vehicles, in contradistinction to all other sorts of containers that might be situated within the curtilage of a dwelling when a search warrant is executed.

[49] Regardless of which solution is chosen, the question arises whether to change the general definition of dwelling-house that appears in section 2 of the *Criminal Code*, or instead to follow a more limited approach.

[50] Changing the section 2 definition would have effects on other sections of the *Criminal Code* that rely on the definition of dwelling-house. For example, breaking and entering is a more serious crime when the subject building is a dwelling-house, with potential liability to imprisonment for life, whereas breaking and entering other premises attracts a maximum of 10 years' imprisonment.[29] In the view of the Working Group, the

---

[25] *Charles*, 2012 ONSC 2001 at para. 61; *R. v. Vu*, 2013 SCC 60 at para. 39.

[26] *R. v. Vu*, 2011 BCCA 536 at para. 47, citing the "elephant in the matchbox doctrine" – a warrant to search for a thing does not authorize police to look in a container that could not contain that thing; *R. v. Owen*, 2017 ONCJ 729 at para. 150.

[27] *R. v. N.N.M.*, 2007 CanLII 31570 (Ont. S.C.J.) at para. 363, citing *Sleeth v. Hurlbert* (1896), 25 S.C.R. 620 at 625-26.

[28] Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at p. 123.

[29] See *Criminal Code* sections 348 and 348.1. Further examples where a change to the

changes to the boundaries of criminal liability that would result from amending the section 2 definition make it an undesirable means of clarifying the question of searching motor vehicles within curtilage.

[51] A more precise solution is to locate a modified definition within Part XV of the *Criminal Code*, or within section 487 itself. Such an approach was taken in the *Cannabis Act* where, for purposes of a specific section only, "dwelling-house" was given a more precise definition. Section 12 of the *Cannabis Act* deals with the number of plants that may lawfully be cultivated within a dwelling-house. Subsection 12(8) states:

> (8) For the purposes of this section, dwelling-house, in respect of an individual, means the dwelling-house where the individual is ordinarily resident and includes
>
> > (a) any land that is subjacent to it and the immediately contiguous land that is attributable to it, including a yard, garden or any similar land; and
> >
> > (b) any building or structure on any land referred to in paragraph (a).

This definition codifies and arguably extends the common law meaning of curtilage,[30] for purposes of that section only.[31]

[52] The Working Group's preferred approach is similar to that taken in section 12 of the *Cannabis Act*: Parliament should create a purpose-specific definition that modifies the meaning of "dwelling-house" (or "building") in the context of search warrants, but does not change the general definition in the *Criminal Code*. For example Part XV of the *Criminal Code* could provide that, for the purpose of any warrant authorizing search or seizure, "dwelling-house" either includes, or does not include, a motor vehicle located within the curtilage of the dwelling-house.

---

section 2 definition of "dwelling-house" would affect the operation of other provisions including *Criminal Code* subsection 83.14(9) and section 490.41 (both dealing with forfeiture of offence-related property that is a dwelling-house); sections 529-529.4 (arrests within a dwelling-house); and various parts of the *Cannabis Act* that rely on the *Criminal Code* definition.

[30] Some, but not all, cases have held that the common law meaning of curtilage does not include the entirety of the yard outside a house. See notes 20 and 21 above.

[31] For all other purposes in the *Cannabis Act*, the *Criminal Code* definition of "dwelling-house" applies: *Cannabis Act* section 2.

[53] Alternately, the new definition of "place" proposed in Part 3.1 above could be further developed to state one of these alternatives:

> In this Part, "place" includes a building, receptacle, or conveyance as defined in section 320.11, and includes any conveyance located within the curtilage of a building.
>
> *or*
>
> In this Part, "place" includes a building, receptacle, or conveyance as defined in section 320.11, but does not include any conveyance located outside a building but within its curtilage unless that conveyance is specifically described in the warrant.

[54] Another drafting approach could avoid altogether the common law concept of curtilage, and instead refer to "a conveyance located outside a building but within the property boundaries of the land on which the building is located," or some similar formulation. There may be advantage in avoiding the common law term "curtilage" which, as noted, sometimes leads to debates about how far the curtilage reaches.[32]

[55] Whichever solution is adopted, consideration should also be given to whether the rule should apply to "motor vehicles," a term which is defined in section 2 of the *Criminal Code*,[33] or to "conveyances," which is defined in section 320.11.[34] Conveyances constitute a larger category: for example, a boat on a boat trailer parked on the driveway beside a dwelling would be captured by a rule that applies to "conveyances," but would not be captured by a rule that applies only to "motor vehicles."

---

[32] See cases cited at note 21 above.

[33] *Criminal Code* section 2: "motor vehicle" means a vehicle that is drawn, propelled or driven by any means other than muscular power, but does not include railway equipment.

[34] *Criminal Code* section 320.11: "conveyance" means a motor vehicle, a vessel, an aircraft or railway equipment.

Recommendation 2:

The Working Group recommends that the confusing state of law about vehicles within curtilage should be clarified. This could be accomplished if the definition of "dwelling-house" is amended, or a definition of "place" is added, in relation to search warrants only, to clarify whether or not a dwelling-house (or building) includes a motor vehicle (or conveyance) located within the curtilage but outside the building or connected structures.

3.3 Bodily searches of people at the place to be searched

[56] It is arguable that section 487 currently does not provide authority for police to conduct a bodily search of a person who is in the place to be searched, even if police have a reasonable basis for thinking that a thing to be seized is within the personal possession of that person.[35] The argument is simply that a person is not a "place" to be searched.[36] However, there does not seem to be authoritative jurisprudence that directly decides this point.

[57] This uncertainty around the reach of a 487 warrant means, for example, that if police obtain a 487 warrant to enter and search a place for a particular cell phone, and police enter under the warrant, and meet a person who has that cell phone in their pocket or in their hand, it may be arguable that the warrant does *not* provide authority to seize the cell phone from the person – even though the warrant authorized police to be in the place, to search for and seize that very cell phone.

[58] In some cases, police might also have grounds to arrest the person, and then could rely on the common law power to search the person incident to the arrest in order to find evidence of the offence for which they are being arrested. But the person holding the evidence is not always a person who can be arrested. Nor is it always desirable to arrest the person, even if they are technically arrestable. (Police may not be ready to lay charges. Or police may not think that arresting is necessary to bring the person before the court, and therefore prefer to use another means of compelling appearance that is less intrusive of the person's liberty.) Search incident to arrest is at best a partial solution.

---

[35] *R. v. Kitaitchik* (2002), 161 O.A.C. 169 (C.A.) at para. 19; Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at pp. 100, 411.

[36] *R. v. Stillman*, [1997] 1 S.C.R. 607 at para. 26. Similarly, it has been held that a person is not a "place" within the meaning of section 489(2): *R. v. Ricciardi*, 2017 ONSC 2105 at paras. 44-45.

[59] Further, when an electronic device is seized incident to arrest, it is important to appreciate that the Supreme Court of Canada established in *R. v. Vu* that only a warrant which specifically anticipates the device will be examined for its data is authority to obtain the data.[37] This means that a search incident to arrest is *not* authority to examine a device for data (beyond the very limited examination that might be permitted incident to arrest under *R. v. Fearon*[38]). Thus, even if police have a *Vu*-compliant warrant for the cell phone, authorizing police to access its data, when police seize that same phone incident to arrest, instead of pursuant to the 487 warrant, it is arguable that police may not access the phone's data (except as allowed by *Fearon*). Because of this uncertainty, it is common in some jurisdictions that police will seize the phone incident to arrest (*i.e.* not relying on the search warrant), then apply for a second warrant to authorize re-seizing the phone they have already seized, for the sake of complying with *Vu*. This approach means police are obtaining multiple warrants for essentially the same search, for a purely technical reason, which does not advance the interests of the accused or of the administration of justice.

[60] Alternatively, police might in some cases be able to rely on exigent circumstances to search the person found at the scene without warrant, assuming police are able to articulate all the grounds that would be necessary to obtain a general warrant under section 487.01 authorizing a bodily search,[39] *and* can justify why there is urgency to conduct the search, based on the risk of loss or destruction of evidence or harm to a person which cannot wait for police to obtain the general warrant.[40] Again, this is at best a partial solution. Further, the exigent circumstances doctrine is meant to only authorize police to act without warrant as is necessary to address the exigency. That is (to continue the cell phone example), once police have seized the phone based on exigency plus suf-

---

[37] *R. v. Vu*, 2013 SCC 60 at paras. 47-49.

[38] *R. v. Fearon*, 2014 SCC 77 at para 83.

[39] A general warrant under section 487.01 can authorize the search of a person, provided the search does not interfere with bodily integrity (subsection 487.01(2)): *R. v. Kitaitchik* (2002), 161 O.A.C. 169 (C.A.) at para. 19; *R. v. Sam*, 2003 CanLII 15852 (Ont. S.C.J.) at paras. 21-23; *R. v. Hamadeh*, 2011 ONSC 1241 at para. 157.

[40] *R. v. Sam*, 2003 CanLII 15852 (Ont. S.C.J.) at paras. 23-31; *R. v. Hamadeh*, 2011 ONSC 1241 at paras. 158-74. Although section 487.11 of the *Criminal Code* does not refer to searches that would otherwise require a general warrant, the common law doctrine of exigent circumstances remains available for searches that normally require judicial preauthorization and that do not have a statutory exigency power: *R. v. Bakal*, 2021 ONCA 584 at paras. 18-33; *R. v. Campbell*, 2022 ONCA 666 at paras. 79-84.

ficient grounds that a general warrant could have been obtained, the exigency will usually have ended because the evidence will have been preserved.[41] Meaning that police would then be required to apply again for a new *Vu*-compliant search warrant to re-seize the phone and access its data – even though police already had such a warrant. This need for repeated warrants, where one should be sufficient, clearly points to the need for reform.

[61] There is a better solution, already found in Federal criminal law. The search warrant provisions in both subsection 11(5) of the *Controlled Drugs and Substances Act*, and in subsection 87(5) of the *Cannabis Act* provide that when police are in a place, executing a warrant to search for and seize things listed on the warrant, and an officer reasonably believes that one of the things to be seized is in the personal possession of a person who is in the place, then police may search the person for the thing.

[62] Returning to the cell phone example again: if police obtain and execute a *Vu*-compliant *CDSA* search warrant for a controlled substance and for a cell phone (relying on *CDSA* paragraphs 11(1)(a) and (d)), police can search anywhere in the place where the drugs or the phone might be located, *and*, if an officer additionally has a reasonable belief that either drugs or phone are in the personal possession of someone found at the place, police can additionally search the person for the drugs or the phone. If the cell phone is then seized from the person, police can go on to access its data pursuant to the terms of the *CDSA* search warrant. Unlike with the arguably more limited 487 warrant, there would be no need to obtain a second, *Vu*-compliant warrant, since the first warrant would both authorize the seizure of the phone from the person and would contain *Vu*-compliant terms allowing for police to access the data in the phone.

---

[41] *R. v. Lucas*, [2009] O.J. No. 3417 (S.C.J.) at para. 26, aff'd 2014 ONCA 561 at para. 237; *R. v. Kelsy*, 2011 ONCA 605 at para. 35 ("By their nature, exigent circumstances are extraordinary and should be invoked to justify violation of a person's privacy only where necessary"), citing *R. v. Feeney*, [1997] 2 S.C.R. 13 at para. 52; Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at p. 405.

Recommendation 3:

The Working Group recommends that section 487 of the *Criminal Code* be amended to add a provision analogous to subsection 11(5) of the *Controlled Drugs and Substances Act* and subsection 87(5) of the *Cannabis Act*, to clearly allow for searches of persons found at the place to be searched, when an officer has reasonable grounds to believe they have on their person one of the things authorized to be seized under the search warrant.

3.4 Entering a place to make observations and measurements

[63] It is well established that police are implicitly authorized to document the conduct of a warranted search, including by the making of photographs and video recordings.[42] However, a 487 warrant is *not* capable of authorizing entry into a place when the purpose of the entry is to take photos, videos, or measurements. This is because those activities do not constitute the search of a place *to seize a thing*. The 487 warrant does not authorize searching for or seizing intangibles like photographs or video recordings.[43]

[64] If police want to enter a place for the purpose of taking photos, videos, measurements, or similar techniques that are not predominantly aimed at seizing a thing, then police currently must seek a general warrant under section 487.01. As noted earlier, it is more procedurally onerous for police to obtain a general warrant than it is to obtain a 487 warrant. In the context of entering a place to make and record observations, the additional burden of seeking a general warrant does not seem justified. The level of intrusion on individual rights from entering to make and record observations is no greater than the level of intrusion caused by entering and searching for things under a 487 warrant. Hasan *et al.* argue, in *Search and Seizure*:

---

[42] *Euro-Can-Am Trading Inc. v Ontario (AG)*, 1997 CanLII 1288 (Ont. C.A.) at para. 15: ("In our opinion the audio/videotape was nothing more than a record of the search and seizure that would be admissible if required to show how and where the search was conducted"); Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at pp. 102-03. Also see *R. v. A.H.*, 2018 ONCA 677 at paras. 28, 41 (police could take photos to document a warrantless seizure under section 489(2)); *R. v. Montgomery*, 2013 BCSC 1010 at para. 39, and *R. v. Ceballo*, 2019 ONSC 4617 at para. 60 (police could document a warrantless search conducted incident to arrest).

[43] *Quebec (A.G.) v. Royal Bank of Canada et al.* (1985), 18 C.C.C. (3d) 98 (Que. C.A.) at 100; *R. v. Wong* (1987), 34 C.C.C. (3d) 51 (Ont. C.A.) at 61 ("…a search warrant cannot be issued for intangible objects. It is hard to imagine anything more intangible than the ephemeral, flickering video reproduction of a human action."), aff'd [1990] 3 S.C.R. 36.

> … From a privacy perspective, if an ordinary section 487 warrant can authorize the search of a location and the seizure of tangible things of evidentiary value based on "reasonable belief," there is no reason that it should not also be able to authorize the search of the same location and the creation of intangible photos, videos, measurement, or diagrams based on "reasonable belief." The latter techniques are no more invasive than the former. Indeed a credible argument can be made that they are *less invasive* because they result in less inconvenience to the affected individual.
>
> Nevertheless, until section 487 is amended to specifically allow for authorization to create photos, videos, measurements, and diagrams, the police, counsel, and judges are stuck with the requirement for a general warrant in cases where police wish to employ these investigative techniques without searching for and seizing tangible things.[44]

[65] The Working Group endorses this comment and recommends that section 487 be amended to allow for police to enter and make observations, photos, video recordings, and other measurements of a place and of things found therein.

[66] The recognized authority of police to document the execution of a warranted search by means of photography, video or other means, should be maintained. The proposed amendment should indicate, for greater certainty, that the existing authority of police to document the execution of a warranted search is not affected.

Recommendation 4.1:

The Working Group recommends that the nature of the entry and search capable of being authorized by a *Criminal Code* 487 warrant be expanded, to allow for police to enter a place in order to make observations of the place and of things found therein that there are reasonable grounds to believe will afford evidence of an offence, and to document those observations, including by way of photographs, video recordings, and other measurements, without a precondition that police search for and seize any tangible thing. The amendment should indicate that the existing authority of police to document the execution of a warranted search is not affected.

[67] The Working Group also considered whether there should be a role for technology to augment or extend the view of officers who execute warrants to enter and make

[44] Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at p. 105 (emphasis in original; internal citation omitted).

observations. The current section 487 provides for search warrants "authorizing a peace officer or public officer" to enter and search a building, receptacle, or place. It is arguable that under the current provision, an officer must physically enter the place with their body, thus searching by remote technological means is not within the scope of authority provided by a 487 warrant. When the original search warrant provision was enacted in 1892, nobody would doubt the proposition that an officer's body must enter the place in order to execute a search warrant. In 2023, the Working Group thought it appropriate to consider whether a modernized provision should clarify whether tools for remote presence are within the scope of a warrant to enter and observe a place. That is, should police be understood to have entered the place to be observed if they do so remotely, by technological means, without the officer's body physically entering the place?

[68] A useful comparison can be made to the entry and inspection powers in the *Tobacco and Vaping Product Act* (S.C. 1997, c. 13, as amended (*TVPA*). Those powers were amended in 2018 to provide that inspectors enter a place "when they access it remotely by means of a telecommunication": subsection 35(3). The *TVPA* further provides that when an inspector enters a place by such means, if the place is not accessible to the public then the inspector must enter "with the knowledge of the owner or person in charge of the place" and only for so long as is necessary to conduct the inspection: subsection 35(4). In other words, an entry by means of telecommunication must be done overtly, not covertly, and must not continue beyond the duration of the authority to inspect.

[69] The Working Group recommends that a comparable provision be enacted in relation to the entry and observation authority proposed above. It should be within the authority of the issuing justice to allow an officer to enter a place by means of a telecommunication, in order to conduct and document observations of the place and things therein.

[70] It is well known that the safety of occupants, bystanders, and police officers is sometimes put at risk when police officers enter a place to execute a warrant.[45] There would be significant benefits from providing for a warrant that authorizes police to overtly but remotely enter and observe a place and the things within. It would reduce the

---

[45] *E.g., Eccles v. Bourque et al.*, [1975] 2 S.C.R. 739 at 749: "Except in exigent circumstances, the police officers must make an announcement prior to entry. There are compelling considerations for this. An unexpected intrusion of a man's property can give rise to violent incidents. It is in the interests of the personal safety of the householder and the police as well as respect for the privacy of the individual that the law requires, prior to entrance for search or arrest, that a police officer identify himself and request admittance." (emphasis added)

chances of injury and death that arise when an occupant seeks to resist a search, and officers respond with potentially lethal force. It would assist in avoiding unnecessary human exposure to hazardous conditions (chemical, biological, or electrical hazards, for example), such as can be present in illicit drug laboratories or industrial sites. And, provided that the remote means of entry is overt, the privacy intrusion should be no greater than if officers entered in person.

[71] The Working Group considered it unwise to attempt to be more specific about the technology used to carry out the remote entry and observation. The Working Group's discussion envisioned officers controlling mobile remote cameras. But technologies change quickly, and it is hoped that the wording "by means of a telecommunication" or something similar will be sufficiently flexible to remain useful well into the future.

[72] A concern was raised about whether the scope of "place" would include computer systems, such that the proposed power could authorize police to remotely access computer systems by means of telecommunication. In answer to that concern, the present recommendation is meant only to address entry into physical places, not virtual places like computers. Part 3.6 of this report addresses remote access to computer systems.

[73] Another concern that arose was whether this recommendation could result in a new *covert* surveillance power. While there is a place for lawful covert surveillance,[46] this Working Group considered such discussions to be outside of its mandate. This report addresses only *overt* search authorities. To ensure that the remote entry is overt, a mandatory version of the "knock and announce" rule should be incorporated into the provision that allows for remote entry by means of telecommunication. The recognized rationales for "no knock" entries involve concerns about risk to personal safety and risk of loss or destruction of tangible evidence.[47] Neither concern arises when the objective is to enter by means of telecommunication to make observations. (The Working Group does not propose any change to the common law rule about "knock and announce" and "no knock" searches that are conducted in person, as opposed to by remote means.)

---

[46] If police seek authorization for covert surveillance methods, those methods are potentially capable of being authorized under section 487.01 and/or Part VI of the *Criminal Code*.

[47] "Knock and announce" before entry is presumptively required by common law in the execution of a 487 warrant, although the common law also permits "no knock" entries where police have reasonable grounds to be concerned about the possibility of harm to themselves or occupants or about the destruction of evidence: *R. v. Cornell*, 2010 SCC 31.

Recommendation 4.2:

The Working Group recommends that the enter-to-observe authority in recommendation 4.1 should provide that officers may enter and observe by accessing the place remotely, by means of telecommunication. Entry and observation by means of telecommunication should include a mandatory condition of execution that police announce the entry, to ensure the observations are conducted overtly.

3.5 Authority for examination of data within or available to a seized computer

[74] The preceding recommendations are connected to the traditional understanding that a search involves entering a private physical space — that is, that a search engages a *territorial* or a *bodily* privacy interest. The next several recommendations move away from that traditional perspective and deal with investigative steps that would, if not authorized, violate a person's *informational* privacy without necessarily being connected to an entry into any physical place.[48]

[75] When police seize an object under a criminal law seizure power (whether judicially pre-authorized or warrantless), the general rule is that police may examine, analyze, and derive information from that object in any manner that is reasonable, at any time while the object is lawfully seized.[49]

[76] However, Canadian jurisprudence carves out certain special situations where the general rule does not apply unless the intrusion on informational privacy is specifically pre-authorized by warrant. Most prominently, the Supreme Court of Canada has held that a person can maintain a reasonable expectation of privacy in computer data even after police have lawfully seized the physical object that holds a representation of the

---

[48] These three overlapping categories of privacy — territorial, bodily, and informational — have been referred to repeatedly in Supreme Court of Canada jurisprudence, starting with *R. v. Dyment*, [1988] 2 S.C.R. 417 at 428, and then in *R. v. Plant*, [1993] 3 S.C.R. 281 at 292, *R. v. Tessling*, 2004 SCC 67 at paras. 19-24, *R. v. Spencer*, 2014 SCC 43 at para. 35, among others.

[49] *R. v. Vu*, 2013 SCC 60 at para. 23: "I accept the general proposition… that "[a] warrant authorizing a search of a specific location for specific things confers on those executing that warrant the authority to conduct a reasonable examination of anything at that location within which the specified things might be found" (Cromwell J.). Also see *Canada (A.G.) v. Foster* (2006), 217 O.A.C. 173 (C.A.) at para. 37; *R. v. Oland*, 2015 NBQB 243 at paras. 181-206, aff'd 2016 NBCA 58 at para. 39 (reversing on other grounds); *R. v. Fedan*, 2016 BCCA 26 at para. 73; *R. v. Strong*, 2020 ONSC 7528 at para. 91b.

data. Consequently, in the special context of computers, police need some form of specific lawful authority to obtain access to such computer data, over and above the authority to seize the physical object.[50]

[77] There is currently no form of judicial pre-authorization designed to address a purely informational intrusion on privacy that arises from examining a seized computer. Absent a purpose-built tool, when authority is necessary the current practice is to use a 487 warrant to confer authority for police to examine or analyze the seized thing. This solution is not ideal. Section 487 is designed around searching places to seize tangible, physical things; it is not designed for authorizing informational searches and seizures. Using section 487 for this purpose leads to several uncertainties about how the section should apply: in particular, what is the "place" to be searched, and what is the "thing" to be seized. Using section 487 also interacts awkwardly with the statutory scheme for reports and continued detention in respect of seized things, pursuant to sections 489.1 and 490. Using section 487 to authorize post-seizure examinations is akin to fitting a square peg into a round hole – it can be done, but the fit is imperfect.

[78] It is worth reviewing the relationship of sections 489.1 and 490 to the search warrant authority. Police can lawfully seize property in a variety of ways, with pre-judicial authorization under a 487 warrant or other specialized warrant, or without a warrant via sections 487.11 (exigency) or 489 (plain view) or under common law authorities like search incident to arrest. With the exception of the search warrant, these other authorities for lawful seizure are not subject to judicial oversight until after the seizure. Whether pre-authorized or not, any seizure under one of these authorities must be dealt with in the same manner under section 489.1, which requires a report to justice any time a thing has been seized using a criminal law authority.[51] This provision requires that the seizure

---

[50] The idea that, in special circumstances, a residual expectation of information privacy could persist after police validly seize the physical object is not unique to computers. In *R. v. Stillman*, [1997] 1 S.C.R. 607, it was held that when a person is in police custody involuntarily, they do not truly abandon their information privacy interest in their DNA contained in discarded biological matter. This is so even though the same act of abandoning biological matter when *not* in police custody is traditionally understood to constitute abandonment of any related privacy interest. See *R. v. Stillman* at para. 62, and *R. v. Patrick*, 2009 SCC 17 at paras. 21, 54-55. Currently, when there is a residual expectation of privacy in a seized biological sample, police can overcome it by re-seizing the material through a search warrant, as was suggested in *Stillman* (para. 128). As this is a relatively rare situation, the working group has elected not to make recommendations about a special examination authority for DNA discarded while in custody.

[51] When a police officer receives a thing by consent of a person entitled to give it, they have not exercised a seizure power, and thus need not make a report to a justice: Scott C.

be reported to a judicial official. Section 489.1 engages and complements section 490, which governs the continued detention and eventual disposition of the seized property. Section 489.1 was added to the *Criminal Code* in 1985 to increase the accountability of police and to ensure that there is a record of all property seized by the state. It was designed to work in conjunction with section 490, which provides a legal mechanism for judicial supervision over tangible seized property. These two provisions, which were designed for the management of seized property in which a search subject has a proprietary interest, fail both conceptually and practically when applied to the seizure of data. Some of these failures are discussed below.

The *Vu* exception

[79] The Supreme Court of Canada's decision *R. v. Vu* acknowledged the general rule that seizure of a thing implies authority to examine and analyse that thing, but it created an exception from the general rule when the subject of the examination or analysis is a computer and its data. The Court held the nature and scope of data stored in a digital computer is potentially so invasive that authority to examine the data stored in the computer cannot be assumed to have been granted by a warrant to seize the physical device. Rather, the justice who issues a warrant to seize a computer must have specifically adverted to and authorized the examination of data in the computer — absent which, the examination is not authorized by the warrant.[52]

The current response to the *Vu* exception

[80] Currently, if police have seized a digital device and want to conduct an examination of that device for its informational content, then police will seek a new warrant to authorize the examination.[53]

[81] The correct form of warrant to be used is, however, not obvious. There was historically a debate about whether a general warrant under section 487.01 was necessary to provide authority for examining a computer already in police custody (on the thinking

---

Hutchison, *Hutchison's Search Warrant Manual, 2020* (Toronto: Thomson Reuters) at p. 356.

[52] *R. v. Vu*, 2013 SCC 60 at paras. 46-49. And similarly, in the context of seizures of computers and phones incident to arrest, the warrantless search and seizure power has also been restricted: *R. v. Fearon*, 2017 SCC 77 at paras. 58 and 83.

[53] As was recommended in *R. v. Vu*, 2013 SCC 60 at para. 49.

that it would be improper for police to seek a search warrant to search their own premises). That view has largely been rejected.[54] Now, the warrant usually takes the form of a new 487 warrant, drafted either to authorize re-seizing the computer that is already in police possession, as the "thing" to be seized and then examined post-seizure;[55] or, to authorize searching the computer as the "place" to be searched for data that are "things" to be seized.[56] That is, police need to choose whether to characterise the computer as the "thing" or as the "place." As Hasan *et al*. point out, it is a false dichotomy: "the most conceptually pure approach may be that a computer is neither a place nor a thing."[57] However given that section 487 is the tool available, there currently is no third option available to police. As will be developed below, the Working Group recommends the creation of a more suitable third option.

[82] Either choice within the place/thing dichotomy has consequences. First, it affects the timing of when the examination of data may be conducted. Under a 487 search warrant, police must enter the "place" within the time stated on the face of the warrant,[58] and must exit the place once the search is concluded.[59] However, examination of the "thing" can continue anytime after seizure, provided the thing continues to be lawfully detained.[60] The implications can be significant: in the case of *Nurse*, the Ontario Court of Appeal confirmed that a Blackberry device, seized as a "thing" under a search warrant, could be re-examined with better tools a year after the initial seizure even though

---

[54] *R. v. Villaroman*, 2018 ABCA 220 at paras. 5 and 21.

[55] *E.g. R. v. Brown*¸ 2019 ONSC 5032 at paras. 10-17, holding that police were entitled to treat a previously seized computer, located in a police evidence locker, as the "thing" to be seized under a new search warrant, and therefore a justice of the peace erred by insisting police must treat the computer as the "place" to be searched.

[56] *E.g.*: *R. v. K.Z.*, 2014 ABQB 235 at paras. 32-33, holding that a computer already in police custody is the "place" to be searched.

[57] Hasan, Lai, Schermbrucker, Schwartz, *Search and Seizure* (Emond, 2021) at p. 353.

[58] *R. v. Woodall*, [1991] O.J. No. 3563 (Gen. Div.) at paras. 57-61, aff'd [1993] O.J. No. 4001 (C.A.) at para. 2; *R. v. Brown*, 2010 ONSC 2280 at paras. 17-23; *R. v. Rafferty*, 2012 ONSC 703 at paras. 26-28; *R. v. Gerlitz*, 2013 ABQB 624 at paras. 61-71.

[59] *R. v. Finlay & Grellette* (1985), 23 C.C.C. (3d) 48 (Ont. C.A.) at 63, [1985] O.J. No. 2680 at para. 66; *R. v. Coull & Dawe* (1986), 33 C.C.C. (3d) 186 (B.C.C.A.) at 189-90, [1986] B.C.J. No. 1338 at para. 13; *R. v. Shin*, 2015 ONCA 189 at paras. 24-25, 34, 57-62.

[60] *R. v. Weir*, 2001 ABCA181 at paras. 18-19; *R. v. Ballendine*, 2011 BCCA 221 at paras. 64-70; *R. v. John*, [2016] O.J. No. 2787, aff'd 2018 ONCA 702; *R. v. Nurse*, 2014 ONSC 1779 at paras. 41-53, aff'd 2019 ONCA 260 at paras. 119-143.

the search warrant had long since expired.[61] This result followed because the timing of the post-seizure examination was not limited by the time for execution of the search warrant. However, if the Blackberry had instead been searched as a "place" under the search warrant, with data to be seized as "things," then police would have lacked authority to conduct the second examination that yielded important evidence in the murder investigation.

[83] Second, characterizing the "place" and the "thing" will affect how the post-seizure procedures under section 490 apply to the seizure. When a computer is seized initially under a *Vu*-compliant 487 warrant, then the seizure of the physical object will be reported under section 489.1 and it will presumably be ordered detained under section 490. The post-seizure examination of it for data can happen after seizure (see *Nurse* cited above). However, if instead the computer is seized by warrantless means, such as a search incident to arrest, then a *Vu*-compliant warrant will still need to be obtained. The initial warrantless search will be reported under section 489.1 and detention ordered under section 490. Then the second seizure under the warrant will also trigger a reporting obligation under section 489.1. Practices and interpretations of that obligation vary across the country, depending in part on whether the second seizure treats the computer as the "place" or as the "thing,"[62] and depending also on whether courts in that jurisdiction consider data to be "things" regardless of their characterization in the warrant.[63] These interpretive uncertainties and regional disparities both point to the need for reform. The *Vu* decision from the Supreme Court of Canada dictates that lawfully seizing a computer is not license to "scour" its data "indiscriminately."[64] Instead, the intrusion of information privacy must be reasonably connected to finding evidence of the offence. The typical method for limiting the scope of examination of computer data is to impose terms in the warrant that speak to the manner or scope of examination that is authorized. A representative example was considered in the case of *R. v. John*, where the 487 warrant

---

[61] *R. v. Nurse*, 2019 ONCA 260 at paras. 119-143.

[62] See, *e.g.,* the contrasting results in *R. v. K.Z.*, 2014 ABQB 235 at paras. 32-33 (holding that that a computer already in police custody should be treated as the "place" to be searched) versus in *R. v. Brown*, 2019 ONSC 5032 at paras. 10-17 (holding that police were free to treat the computer in the evidence locker as the "thing" to be seized, and a justice of the peace erred by ruling otherwise). Members of the Working Group are aware that practices are not uniform either in Alberta or in Ontario.

[63] See the discussion of *R. v. Robinson*, 2021 ONSC 2446, and *R. v. Teixeira,* 2022 BCSC 344, at paragraph 95.

[64] *R. v. Vu*, 2013 SCC 60 at paras. 59-62.

included these terms:[65]

> Once seized, Items 1 and 2 will undergo a computer forensic examination. The examination and analysis will be based on the offences set out in this warrant and will be conducted in relation to the following data:
>
> - Data relating to child pornography as defined by the *Criminal Code*.
> - Data relating to the Gnutella 2 Peer to Peer Network.
> - Data relating to use, ownership an access of the seized items.
> - Data relating to the configuration of the seized items.

[84] On this model, the warrant includes terms that allow examination only for certain categories of data. Those terms are supported by evidence in the ITO establishing the affiant's reasonable belief that the identified categories of data will afford evidence of the offence identified in the warrant. Thus the *Hunter v. Southam* standard of reasonable grounds for belief is applied both to the physical search of the place for the thing, and to the examination of the thing for its relevant informational content. This model of prescribing limiting terms to control the scope of examination allows police flexibility in the methods to be used, but at the same time puts boundaries around what police can and cannot do. In *Vu*, the Supreme Court of Canada rejected a more fine-grained approach to pre-authorization, which would have required that a "search protocol" be set out in advance in any warrant that authorizes police to seek computer data. The Court held that it would be asking too much for police and the issuing justice to foresee all the steps that police will need to follow to seek out relevant data that will afford evidence of the offence. This approach, of prescribing limits on the scope of examination but not necessarily imposing fine-grained procedural protocols, should be carried into a new purpose-built examination authority.

[85] Finally, existing subsections 490(13) and (14) allow police to make copies of seized documents for detention indefinitely, without any need for orders authorizing continued detention. While the related privacy interest in the continued detention of data is discussed later in this report, the existence of these provisions is another example of how ill-suited the regime is to the management of "things" for which a person has no proprietary interest, given explicit provisions allowing for continued and indefinite detention of copies. Because seized data is almost always copied, and given the existence of subsections (13) and (14), it begs the question: to what purpose is section 490 applied in relation to the management of seized data? The Working Group recommends instead that a new authority should be created for preauthorizing seizures of data (recommendation 5.1), and that a new and distinct scheme should apply to the supervision of seized data (recommendation 5.2).

---

[65] *R. v. John*, [2016] O.J. No. 7287 (S.C.J.) at paras. 33-41, aff'd 2018 ONCA 702.

Recommendations for a new examination warrant

[86] The Working Group recommends the creation of a specific authority for preauthorizing examination of a computer for its data.[66] To be clear, this new authority should not be required for every kind of post-seizure examination. The usual common law rule[67] should remain the rule, except in contexts where the law dictates that there is a remaining informational privacy right inherent to an object that has been lawfully seized.

[87] This examination authority should be available to be authorized either at the same time a search warrant issues, or later. Sometimes police will know at the time of seeking a search warrant that they intend to seize and examine computers. In that scenario, police would seek authority to both seize computers and examine them for data, as part of the same combined application. However in many other scenarios police will either not know that computers will be seized,[68] or will not at that time be able to put forward grounds to justify examination of data. The current assistance order provision, section 487.02, is analogous. An assistance order can be granted at the same time as the warrant to which it relates, or can be granted separately, after police discover that an order is needed to compel a third party to assist in giving effect to the warrant.

[88] The new examination authority should also be available without an underlying warrant for entering a place to seize a thing. A routine example arises from search incident to arrest, where the physical seizure of the computer is lawful without warrant, but additional authority to examine arises if police decide they wish to examine the computer for data. Another routine example is when a computer is seized for the purpose of investigating one offence – under a search warrant with terms about the scope of examination that are tailored to that offence – but then discover evidence suggesting another distinct offence. Currently, if police wish to expand the scope of their examination it is necessary

---

[66] "Data" in this report is meant in the broad sense employed by section 487.011 of the *Criminal Code*, which provides: "data means representations, including signs, signals or symbols, that are capable of being understood by an individual or processed by a computer system or other device". Data therefore includes machine code, but also human communications (written, audible, visual), photographs, videos, and any other forms of representational information.

[67] See paragraph 75.

[68] One such example arose from the facts of *Vu*, where police had a warrant to search a house for things that included certain documents, and only upon executing the warrant did they realise that the documents might be in digital form inside a computer.

to obtain a new search warrant.[69] It would be more logical if police could instead obtain an examination authorization for the computer that has already been seized, instead of needing to re-seize the physical object. Similarly, police may validly receive an object by the consent of the owner (thus do not need a warrant for the physical seizure), but still need to seek a new warrant to overcome the informational privacy interests of someone else whose data or communications will be exposed once police examine the object.[70]

[89] Issuance of the authorization to examine or analyze should be supported by reasonable grounds to believe that the examination or analysis will afford evidence of an offence.[71]

[90] Notice of the seizure of data should be given, analogous to the notice of physical seizures that is now required to be given under section 487.093 of the *Criminal Code*, so that an interested person can invoke their rights to seek access to the data, or to seek review of the warrant. In the context of a seizure of a physical device by means of a 487 warrant that is combined with an examination warrant, the necessary notice will be achieved by service of a Form 5.1 notice at the time of seizure of the device, as is now required to be given under section 487.093. However in the case of an examination warrant obtained after the fact, police will need to deliver a second notice so that the person with an interest in the data (if the identity of the person is known) is made aware that police have obtained a warrant to access their data. This notice requirement should not be too onerous, since it will not be feasible in some circumstances for police to ascertain who needs notice, or to find that person. The goal should be to put the person on the same footing as if they had been present when police seized the device, when they would have been entitled to the notice required under section 487.093.

[91] The new notice provision should require that police deliver a written notice reflecting execution of the examination warrant (analogous to Form 5.1) to: (a) the person

---

[69] *R. v. Jones*, 2011 ONCA 632 at para. 36.

[70] In *R. v. Cole*, 2012 SCC 53, an employer validly turned over a computer to police without warrant for purposes of a criminal investigation, but police nevertheless should have obtained a warrant before examining the computer's data because the suspect employee had a reasonable expectation of privacy in his personal activities using the employer's computer. And in *R. v. Marakah*, 2017 SCC 59, it was held that the sender of a private text message may maintain a reasonable expectation of privacy even in the copy of the message residing on the recipient's phone.

[71] Compare *R. v. Vu*, 2013 SCC 60 at para. 48: police "must first satisfy the authorizing justice that they have reasonable grounds to believe that any computers they discover will contain the things they are looking for."

from whom the device was seized, if known, and (b) a person who has asserted an interest in receiving notice about examination of the data, if any, or (c) if there is no person under either of the previous categories, then by delivering the notice to the address of the place from which the device was seized if feasible to do so. Police should be relieved of the obligation to give notice if there is no person to whom notice can be given under any of the three categories mentioned, or if a Form 5.1 notice has already been delivered and that notice adverted to police intending to access the data in the seized device.

[92] Waiver of the notice obligation, if sought, should be sought through the report to a justice: police should identify whether notice has been sent (and to whom and by what means), or should explain why notice could not be given (*i.e.* no person with an interest in the data is known to police or cannot be located), or why notice need not be given (*i.e.* sufficient notice was already given by way of the Form 5.1 at the time the device was seized). Waiver should be capable of being granted by a Justice of the Peace who receives the report if they are satisfied that it is not practicable to deliver the notice under any of the three categories, or that a second notice is not necessary because notice was given previously by a Form 5.1 that adverted to the intention of police to access the data in the device.

[93] The Working Group also considered whether it should be permissible for police to not give notice in order to access the data covertly, but concluded that covert access to data should remain within the realm of section 487.01, the general warrant.

Recommendation 5.1:

The Working Group recommends the creation of a new form of warrant for a specified examination or analysis of computers and computer data. The purpose or scope of examination or analysis should be prescribed in the terms of the warrant. The warrant should be available either in conjunction with a *Criminal Code* 487 warrant, or separately. Pre-conditions for issuance should include that the applicant reasonably believes an offence has been committed, and that the proposed examination or analysis will afford evidence of that offence.

Notice should be given of the examination warrant. When the examination warrant is joined with a *Criminal Code* 487 search and seizure warrant, notice is achieved by means of the Form 5.1 that is required to be given under section 487.093 of the *Criminal Code*; that notice will indicate police have an examination warrant and thus that police intend to access data from the device. However when the examination warrant is obtained after the physical seizure, written notice of the examination warrant should be required to be sent to (a) the person from whom the device was seized, if known, and (b) a person who has asserted an interest in receiving notice about examination of the data, if any, or (c) if there is no person under either of the previous categories, then by delivering the notice to the address of the place from which the device was seized if feasible to do so. Waiver of the notice obligation should be capable of being granted by a Justice of the Peace if police show it is not practicable to give notice, or if sufficient notice has already been given.

[94] Every seizure of a thing using a criminal law power requires a report to a justice, pursuant to section 489.1 of the *Criminal Code*. That report then triggers section 490, entailing ongoing judicial supervision of the continued seizure of the seized thing. Like section 487, the statutory scheme in sections 489.1 and 490 was not drafted with informational seizures in mind. Sections 489.1 and 490 govern the treatment of property held in police custody, but the sections do not address the information stored within seized property. Nothing is removed from the seized device when data is extracted from it to produce a copy; it remains whole. In this sense, data are best considered intangibles rather than "things."[72] The focus of sections 489.1 and 490 is to provide judicial oversight for the treatment of seized property to ensure it is not unjustifiably withheld from its lawful owner. They do not afford any discretion to assess the lawfulness or scope of the seizure, nor whether the terms of the warrant were followed. On this view, so long as the warrant explicitly lists the electronic device as the "thing" to be seized, compliance with sections 489.1 and 490 should not require that data be treated as another "thing" requiring an additional report.

[95] Yet, courts are trying to fit the current *Charter* concept of informational privacy into a statutory scheme that was designed around physical seizures. Consequently, there has developed an unfortunate and confusing split in the jurisprudence respecting how to comply with the obligation to make a report to a justice when police seize intangible

[72] Courts have held that a search warrant cannot be obtained for an intangible that cannot be brought before a justice: *Quebec (A.G.) v. Royal Bank of Canada et al.* (1985), 18 C.C.C. (3d) 98 (Que. C.A.) at 100; *R. v. Lauda*, 1998 CanLII 2776 at para. 26 (Ont. C.A.), aff'd [1998] 2 S.C.R. 683; *R. v. Wong* (1987), 34 C.C.C. (3d) 51 (Ont. C.A.) at 61, aff'd [1990] 3 S.C.R. 36.

information that engages somebody's privacy interests. A representation of that debate is illustrated by the competing decisions of *R. v. Robinson*, 2021 ONSC 2446, and *R. v. Teixeira*, 2022 BCSC 344.[73] The *Robinson* decision, currently binding in Ontario,[74] holds that when the computer is the "thing" to be seized under a search warrant, and police comply with their obligations by reporting the seizure of the physical computer under section 489.1 and obtaining a detention order for the computer under section 490, there is no additional obligation to make a second report to a justice when post-seizure examination of the computer yields data. In contrast, the *Teixeira* decision, currently binding in British Columbia,[75] holds the opposite, saying that despite police complying with sections 489.1 and 490 in respect of the physical computer, a post-seizure examination that yields data requires a new report to a justice about the data. These two interpretations appear to be irreconcilable.[76]

[96] In view of that debate, it is notable that under the current production order scheme,[77] Parliament has explicitly provided that the requirements about reports to a justice and detention orders do *not* apply to copies of documents or data acquired through a production order.[78] This makes sense in relation to copies: nobody has been deprived of possession of the original documents or data, so there is no possessory interest to be protected by returning the copies. And, this is consistent with subsection 490(13) of the

---

[73] *R. v. Robinson* is available only from Quicklaw, at [2021] O.J. No. 1797. *R. v. Teixeira* is currently unreported.

[74] There is a competing decision in Ontario, *R. v. DaCosta and Jeffrey*, 2021 ONSC 6016 at para. 45, which disagrees with *Robinson*. However the court in *DaCosta and Jeffrey* did not apply the "*Spruce Mills* criteria" before departing from a prior decision (*Robinson*) on a point of law from a court of coordinate jurisdiction: *R. v. Sullivan*, 2022 SCC 19 at para. 75. Applying the Supreme Court of Canada's decision in *Sullivan* to resolve the disparity, it appears that *Robinson* represents the current state of the law in Ontario. The *Robinson* decision has been followed in *R. v. Johnson-Phillips et al*., 2023 ONSC 1977 (unreported).

[75] The *Teixeira* ruling has been followed in *R. v. Bottomley*, 2022 BCSC 219 (unreported).

[76] A significant distinction between *Robinson* and *Teixeira* is that in the latter, the warrant specified data as "things" to be seized, and the "place" was described as the police locker and the device in the police locker. On this basis, *Teixeira* may be distinguishable from *Robinson*, which continues to be followed in most jurisdictions outside of B.C.

[77] *Criminal Code* sections 487.011 through 487.0199, enacted in 2014.

[78] Subsection 487.0192(4) states, "For greater certainty, sections 489.1 and 490 do not apply to a document that is produced under an order under any of sections 487.014 to 487.018."

Criminal Code, which provides that when seized documents are returned, police can keep copies.

Recommendations for a new supervisory scheme for data

[97] The recommendation of the Working Group to create a new type of warrant for the examination or analysis of data is also an opportunity to propose a new supervisory scheme applicable specifically to data. A new regime would be better suited to technological reality and would avoid the difficulties that can arise with the current scheme in sections 489.1 and 490. It would also address the growing judicial preoccupation with informational privacy interests,[79] in a time when personal information is increasing stored in remote and distributed digital formats.[80]

[98] The seizure of data, or of a medium containing data, should result in a report to a justice of the peace. This report should be limited to a general description of the data seized. A detailed inventory of the data should not be required; such a requirement would often be impossible to meet within a reasonable timeframe, as the processing times for analysing data can be very long, given the volume of cases, the volume of data seized, and sometimes the need to decrypt the devices or the data. Requiring a detailed inventory could also require accessing data outside the scope of the warrant, which is not desirable in order to comply with section 8 of the *Charter*. The level of detail in the report to a justice should be the same as the level of detail in the notice discussed in recommendation 5.1. The Working Group anticipates that police will generally reproduce the description given in the notice that was delivered (or would have been delivered, but for waiver of the notice obligation) or attach a copy of the notice to the report.

[99] Furthermore, a single report to the justice should be able to account for both the seizure of an electronic device and the data contained therein. This initial report to the Justice of the Peace, whether it is for the physical device and its data or just the data, should be sufficient and no further report should be required. Thus, subsequent analysis of the data should not result in further reports to the Justice of the Peace.

[100] In general, seizing data can be done in two ways. First, the data can be copied to a medium belonging to the police force. In this case, the person from whom it has been

---

[79] The S.C.C. explained in *R. v. J.J.*, 2022 SCC 28 at para. 44: "… Informational privacy protects the ability to control the dissemination of intimate and personal details about oneself that go to one's 'biographical core'. As this Court held in *R. v. Dyment*, [1988] 2 S.C.R. 417, informational privacy is "based on the notion of the dignity and integrity of the individual". [internal citations omitted]

[80] See note 2, above.

seized always has access to the data, since he or she retains the original medium. Secondly, the electronic device on which the data is located can be seized, together with the data it contains. The person from whom it was seized thereafter no longer has access to the data.[81] In the second case, the eventual return of the device will, usually,[82] allow this person to also get their data back. Copies may also be made which are indistinguishable from the original data. In these circumstances, it should not be necessary to obtain a detention order for the data. The physical device should continue to be subject to section 490, but the data should be excluded from the continued detention scheme. The report to the Justice of the Peace should be sufficient to provide judicial oversight of the seizure, if certain access mechanisms are added, as discussed below.

[101] Ideally, this possibility of keeping data without a detention order should only apply to data that is within the scope of the warrant. However, in computer matters, it is often necessary for technical reasons to seize all the data contained in a device and then analyse it to extract what is really the object of the search.[83] The proposed scheme should take this reality into account and allow for the wider data set to be kept for as long as the data may be required for analysis during an investigation. In view of the long lead times for analysis of the data, an initial period of one year could be provided. This period could be renewed by application to a judge[84] if it is demonstrated that the data is still needed for the investigation and proceedings have not yet been initiated. In the same way as in paragraph 490(2)(b) and paragraph 490(3)(b), when legal proceedings are initiated, this data could also be kept without the need for extension orders. Once proceedings are initiated, keeping the data is necessary for reasons of preservation and integrity of the

---

[81] Subject to data that are also accessible by remote means, such as in "cloud" storage.

[82] It could be that the device is never returned to the seized person, for example, if it is confiscated as offence related property. It could also be that the decryption procedure renders the device unusable, or that it has become obsolete between the time of seizure and the time it can be returned to the seized person.

[83] *Uber Canada inc. c. Agence du revenu du Québec*, 2016 QCCS 2158 at para. 262; *Autorité des marchés financiers c. Baazov*, 2018 QCCS 3422, para. 79-82. Also see Orin S. Kerr, "Executing Warrants for Digital Evidence: the Case for Use Restrictions on Nonresponsive Data", 2015, 48 Texas Tech. L. Rev. 1.

[84] The level of judicial official who can authorize keeping the data beyond a year should be the same as the official who can authorize detention under section 490 beyond one year. Currently, only a superior court judge or a section 552 judge (which includes judges of the Court of Québec) can do so. The Working Group reviewing section 490 may be considering a change to paragraph 490(3)(a). If that subsection is changed, this new proposed provision should follow.

evidence, as well as for potential examination by the defence.

[102] It should be made clear that this possibility to keep all data during the investigation is *only* for the purpose of preserving the data and *cannot* be used as a justification for analysing or accessing data outside the scope of the warrant. To access data that are preserved under this provision but outside the scope of the warrant, a new judicial authorization should be required. It should also be made clear that police are required to store the data securely and reliably, so that it remains available if needed by an accused to make full answer and defence or if access is otherwise authorized by a court.

[103] After the conclusion of the proceedings, or after a decision is made not to lay charges, this broader data set should be destroyed or rendered permanently inaccessible unless police first obtain a new order for continued possession of the data. This obligation to destroy should only apply to data that exceeds the scope of the warrant. Prior to destruction, notice should be given to the person to whom notice about the examination warrant was sent, and to any other person who has since declared an interest in receiving notice, to ensure that they can assert the right to request a copy, if they so choose, before destruction.

[104] The person from whom data were seized should be given a way to seek access to the data. Indeed, this is necessary considering that when the physical device and the data are both seized, the person may be deprived of their data. Furthermore, the return of the physical device will not always facilitate retrieval of the data, as sometimes the decryption procedure may render a device unusable or it may have become obsolete with the passage of time since the seizure. The person from whom it was seized, or the rightful owner of the data, should therefore be able to request a copy of, or access to, the data, in whole or in part. The burden that currently exists in subsection 490(8) of the *Criminal Code* could serve as an inspiration for this. The person would have to show that he or she would suffer hardship if access to or a copy of the data cannot be provided. This burden is necessary to filter out frivolous or dilatory requests. The judge should have the power to impose conditions on access or copying. The ability to impose conditions is important, because other people may have privacy interests or proprietary interests in the seized data, and because some kinds of data are illegal to possess (*e.g.* child sexual abuse material, in most circumstances) or to distribute (*e.g.* intimate images, if distributed without consent).

[105] Another mechanism to access data should also be created for any person who has a legal interest in the data. This would not be limited to the person from whom it was seized and could, for example, apply to the accused when they are not the same person, or it could apply to third parties. In order to obtain access or a copy of the data, that person would have to show that this is necessary to enable him or her to pursue his or her legal interest. This mechanism is modelled on subsection 490(15) of the *Criminal*

Code, with some modification. To be clear, this mechanism is *not* about providing disclosure to an accused person, which they are entitled to receive to make full answer and defence (*Charter* section 7; *R. v. Stinchcombe*). Rather, this mechanism would be potentially available when someone (whether an accused person or a third party) has an articulated legal interest in the data outside of their *Stinchcombe* entitlement to disclosure. For example, a litigant in a civil action, or a regulatory agency, might seek access to data that police have seized. Alternately, an accused who has received their *Stinchcombe* disclosure might also seek to rely on this mechanism to obtain access to seized data that is outside the scope of the examination warrant – and therefore beyond what the police and prosecution can disclose. In a case where two or more people are both charged with offences, one accused might seek access to data from the other accused's device, or from a witness's device, beyond what police have obtained pursuant to an examination warrant. In such cases, the privacy interests of other parties will need to be heard before access can be granted – akin to a third-party records application where the privacy-holder receives notice and has standing to assert their privacy rights. Again, access or copying could be total or partial, and the judge should be able to impose whatever conditions he or she considers appropriate.

[106] Finally, as in subsection 490(14) of the *Criminal Code*, copies of the data should have the same evidential value as the "original" data, as long as they are certified as true by the person who made them or that their conformity with the original can be demonstrated in some other way.

[107] The Working Group considered whether there should also be a default rule about destruction of data *within* scope of the examination warrant, once the investigation or court proceedings have concluded.[85] An argument was advanced that police should be required to seek an order to retain any seized data after the conclusion of the case, or especially after an acquittal. Destruction of data obtained by warrant, which police were therefore authorized to use in their investigations, presents difficult challenges. The information police are entitled to access by the warrant may end up in multiple documents throughout an investigative file – summaries, reports, notes, interview plans, witness statements, and so on. It may also be included in court documents (including affidavits in support of further authorizations, and trial exhibits), and may be distributed to other

[85] If the justice who issues a warrant is concerned about data being kept indefinitely, or being used for other investigations, it is always open to the justice to impose limits at the time of issuance. See, *e.g.*, *R. v. Musara*, 2022 ONSC 3190 at para. 200: "If an issuing justice is concerned about the retention of such data, it can be made a term of a search warrant to delete the extracted data after a specified period of time, such as the conclusion of the appeal period after a verdict or any appeal."

parties (the prosecution, the accused). Purging an investigative file of information obtained by warrant would be laborious and impractical. Nor does it seem wise erase history. Sometimes, police are required to be accountable for their investigative work through an appeal brought long after the fact, or through a civil court process or a regulatory review. Sometimes, investigations are reopened. If police were required to purge data after the conclusion of a case, these means of after-the-fact accountability would be frustrated. In the end, the Working Group does not recommend any new rule about destruction of data that was within the scope of the examination warrant. Instead, police investigative files should continue to be dealt with by the archiving and destruction rules applicable under provincial law. Justice Canada may wish to consider creation of a mechanism by which an accused person who is later acquitted could apply for an order requiring destruction of their data in the police file, while bearing in mind the interplay of Federal and Provincial laws in this area.

[108] In summary, the Working Group proposes that data *within* the scope of the examination warrant can be kept as needed. This accords with the current law. Data *outside* the scope of the warrant may also be kept but only under more limited conditions: the duration for which the out-of-scope data may be kept is limited, unless an extension order is obtained or proceedings are instituted. And the purpose for which the out-of-scope data may be kept is strictly limited to preserving it, but not using it, unless a further court order is obtained. The out-of-scope data is subject to destruction after the conclusion of the proceedings, or after keeping it can no longer be justified by police when no proceedings have been initiated. These new limits are more protective of privacy than the existing law, which currently makes no provision for notice of examination of data, nor for destruction of data.

Recommendation 5.2:

The Working Group recommends amending the *Criminal Code* so that when a warrant for the examination or analysis of data is executed, a report must be made to a justice in regard to the seizure of data. Data that is *within* the scope of the warrant should then be allowed to be kept and used by law enforcement.

Any data *outside* the scope of the warrant that was required to be seized should also be kept, for an initial period of one year, renewable, or for so long as necessary after proceedings are instituted. However, this out-of-scope data set should be destroyed within a defined period after the end of the proceedings (with allowance provided for appeal periods), or after a decision is made not to lay charges, unless police first obtain a new order for continued possession of the data.

A mechanism to allow an interested person to access seized data should be provided. Any person with a legal interest in the data should be able to request access if they can demonstrate that access is necessary to advance that legal interest. Access or provision of a copy of data should be subject to any conditions that might be imposed by the court.

Finally, copies of the data should be deemed to have the same evidential value as the data seized if they can be certified as true copies of the data seized by the person who made them or if their conformity can be demonstrated by other means.

[109] Alternatively, in the absence of a new authority for post-seizure examination of a computer for its data, the language in sections 489.1 and 490 in the existing scheme could be amended to make clear that data are not "things" unless specifically characterized as such in the warrant. Additionally, subsection 490(13) could also be amended to clarify that the scope of "document" includes digital information, such that the provision would apply to both physical copies of documents and to copied data from electronic devices. Such an amendment to subsection 490(13) would provide clarity by codifying holdings by multiple courts about the provision applying to both physical documents and electronic data.[86]

3.6 Accessing and copying computer data by remote means

[110] Section 487 was amended, in 1997, to provide certain powers to police for accessing computer data while executing a 487 warrant in a place. Although useful, the 1997 amendments are significantly limited in today's technological environment. They deserve to be updated.

[111] Subsections 487(2.1) and (2.2) provide:

> *Operation of computer system and copying equipment*
>
> **(2.1)** A person authorized under this section to search a computer system in a building or place for data may
>
> (a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;
>
> (b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

[86] *Bromley v. Canada*, 2002 BCSC 149 at para. 26; *R. c. Libby*, 2008 NBBR 36 at paras. 89-91; *Green v. Diack*, 2012 ABQB 45 at para. 147; *R. v. Eddy*, 2016 ABQB 42 at para. 46; *Winnipeg v. Caspian Projects Inc.*, 2021 MBCA 33 at para. 35.

(c) seize the print-out or other output for examination or copying; and

(d) use or cause to be used any copying equipment at the place to make copies of the data.

Duty of person in possession or control

(2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

(a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for;

(b) to obtain a hard copy of the data and to seize it; and

(c) to use or cause to be used any copying equipment at the place to make copies of the data.

[112] As can be seen from the text of the enactment, subsection 487(2.1) remains oriented around authorizing police to carry out certain steps while in a physical place, and then to seize physical things. The first of those limitations — the orientation toward entering and searching places — cause this provision to be little used in practice. The second — the orientation toward generating a physical thing to be seized — is an unnecessary anachronism except for its uncomfortable interplay with the report to justice and property management regime discussed above.

[113] First, while this does not appear to have received judicial consideration, it appears from the text of the enactment that subsection 487(2.1) might only be available to police while they are present in the place to be searched under the 487 warrant. If correct, this means that unless police can identify a place in which computers will be found that contain or have available to them the data sought, the provision is of no utility. Arguably, it may also mean that police must access and copy the data while "on scene" at the place to be searched. If doing so is not practical (for example, if it would be too time-consuming, or if police need specialised tools that were not brought to the scene), then police will need to resort to more intrusive options: either police will stay at the place for as long as it takes to copy the data, thus increasing the inconvenience and intrusion for the rightful occupants of the place, or police will simply seize the computers and take them away for later examination at the police station. Both solutions are more intrusive than would be necessary if the statute provided a better tool that allowed for judicial preauthorization to overtly access a computer system without necessarily searching a physical place.

[114] Second, subsection 487(2.1) requires that police create "a print-out or other intelligible output" for seizure. In practice, police will usually copy data onto a portable digital storage device rather than printing the data onto paper, but either way, the necessity of creating a physical object at all is out of step with current technology. Police should be permitted to copy data onto a device or a remote file server that police already own, without police then being required to seize their own device and subject it to the reporting and detention regime in sections 489.1 and 490.

[115] To address both deficiencies, the Working Group recommends that the authority to access and seize computer data should be updated. In addition to the existing power in subsection 487(2.1), the *Criminal Code* should also provide for a warrant to allow police to copy data that resides in or is available to a computer system that police can remotely access, without needing to identify and then physically enter the place where the computer is located and without needing to generate a physical thing to be seized.

[116] There are several common examples where police may want to seek authorization to obtain and use data not located on a physical medium that police could physically seize:

- A witness might send police a transmission of information (such as an e-mail message) containing electronic copies of documents relating to a suspect.
- A witness might provide a password that gives police access to data stored remotely, or police might obtain the password by other lawful means, and want to use a police computer to gain access to the remote data.
- Police become aware of a trove of private information that has been made available on the internet without the consent of the privacy-holder.

Assuming in each of these examples that someone maintains a reasonable expectation of privacy in the information, then police need some form of legal authority to examine and use it. Yet there is no physical "thing" in relation to which police could obtain a 487 warrant; nor do police need authority to physically enter any physical "place". Currently, any form of judicial preauthorization that can be applied to these common scenarios is an awkward work-around. The time has come for the search warrant provision to grow beyond the 1892 paradigm of searching a place to seize a thing.

[117] Search and seizure of data by remote means is currently authorizable by way of a general warrant, under section 487.01, or alternatively by way of a production order under section 487.014 directed to a third party (*i.e.* someone who is not a suspect in the criminal investigation) who has possession or control of the data. Neither option is ideal.

[118] The case of *Strong* illustrates the method using a general warrant. In that case, police obtained a general warrant pursuant to section 487.01 that authorized a series of procedures, including resetting a password with the compelled assistance of a third party, that ultimately allowed police to log in remotely to the accused's Google e-mail account (a web-based e-mail service) and then search for specified data that were relevant to a murder investigation.[87] Note that the level of the privacy intrusion was *not* what dictated the choice of warrant in the *Strong* case. If police had been able to identify a place to be searched within which was located a computer system that contained or had available to it the data sought, then a normal 487 warrant, issued upon reasonable grounds for belief and relying on subsection 487(2.1), could have authorized the search and seizure of the data, perhaps with an assistance order to require the third party to participate in resetting the password. But, because there was no such physical place to be searched, police needed to resort to the more procedurally onerous general warrant. In other words, the resort to a general warrant was necessary because of a technical legal reason, and not because of a constitutional reason about protecting a reasonable expectation of privacy.

[119] While the *Strong* scenario was a covert search, it nonetheless highlights a gap in the current 487 authority, namely an overt remote search power to be used when police have legally obtained credentials and can remotely access computer system in an overt manner. The Working group proposes that a warrant for remote access to computer data should be created.

[120] A production order, under section 487.014 of the *Criminal Code*, is also a potential tool for obtaining computer data, when data are in the possession or control of a person (including a company) who is not a suspect in the criminal investigation[88] and who is within the jurisdiction of a Canadian court. It appears that even a person who is physically outside of Canada can be made subject to a production order provided they have a "real and substantial connection" to Canada.[89] However, the practical reality is that most companies that provide remote data storage operate outside of Canada, and are subject not just to Canadian laws but also to domestic laws of other sovereign states. The

---

[87] *R. v. Strong*, 2020 ONSC 7528 at paras. 93-120.

[88] Subsection 487.014(4) of the *Criminal Code* excludes the use of a production order against a person who is under investigation for the offence. This respects the right against compelled self-incrimination.

[89] *B.C.(A.G.) v. Brecknell*, 2018 BCCA 5; *Re Application for a Production Order, s. 487.014 of the Criminal Code*, 2019 ONCJ 775; *R. v. Love*, 2022 ABCA 269; *Re textPlus Inc.*, [2022] O.J. No. 4959 (S.C.J.); *Re Service de police de la Ville de Montréal*, 2022 QCCS 3935. *Contra: In the Matter of an application to obtain a Production Order pursuant to section 487.014 of the Criminal Code*, 2018 CanLII 2369 (NLPC)

practical ability of Canadian law enforcement and Canadian courts to obtain compliance from an unwilling foreign company is limited.[90]

[121] Another issue with respect to existing paragraph 487(2.1)(a), that is, "to search any data contained in or available to the computer system", relates to circumstances where the location of the data is not known, for example, in certain dark web scenarios, in situations where the data is stored in the "cloud," or when a computer system has established encrypted tunnels to data storage devices in unknown locations. In these circumstances, arguably, the territorial ambit of the search power may be unknowingly extended outside of Canada.

[122] While caution must be employed when exercising extra-territorial jurisdiction, since the extension of jurisdiction by one state may adversely impact the sovereignty of other affected states, including the rule of law frameworks (the domestic human rights, security, criminal justice and other elements) that derive from sovereignty, it remains that police might not know at the time of the search if they have gone beyond Canadian jurisdiction. Obtaining the consent (or more commonly, participation) of the state where the evidence is located is preferable – and will generally be subject to bilateral, multilateral or international agreements and treaties (*e.g.* Mutual Legal Assistance agreements; Budapest Convention; bi-lateral agreements relating to the US Clarifying Lawful Overseas Use of Data (CLOUD Act); United Nations Convention against Transnational Organized Crime (UNTOC); United Nations Convention against Corruption (UNCAC)).

[123] Nevertheless, many countries have adopted legislation or legal approaches (supported by jurisprudence) to authorize their domestic law enforcement to search (access) and seize (copy) computer data available to a computer in their jurisdiction, regardless of the location of the underlying data files. Examples include Portugal, Netherlands, Belgium, France, Spain and the United Kingdom. While this may solve the issue of domestic legal authority that comes up in these scenarios, it does not address and answer many of the sovereignty issues discussed above.

[124] Resolution of these issues of international law is beyond the reach of this Working Group, but they are noted here for consideration by the drafters of any new legislation in response to the Working Group's recommendations.

---

[90] For example, even a decision by the Supreme Court of Canada in *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34 was not enough to convince a U.S. company to comply with a Canadian court order. Google Inc. instead went to court in California and obtained an injunction against enforcing the Canadian order in the United States. Google Inc. sought to then have the Canadian order revoked, but was unsuccessful: *Equustek Solutions Inc. v Jack*, 2018 BCSC 610.

[125] Keeping in mind that the Working Group's focus is on *overt* search and seizure, a notice requirement is necessary. The notice scheme should be similar to that proposed above in connection with the examination warrant, except that the presumption will be that notice be given, where feasible, by a means that will come to the attention of the person in possession or control of the data that was remotely accessed. The Working Group envisions that police might send an e-mail message to the e-mail account that was accessed, or might leave a written message in some other way, or might contact the person by other written means. The goal should be to put the person who is in possession or control of the data into the same position as if police had obtained access through an examination warrant. Notice should be required to be given forthwith or as soon as practicable after execution of the remote access warrant. And as with the notice required in connection with the examination warrant, this notice obligation should be capable of being waived upon satisfying a justice, in the report to a justice, that giving notice was not practicable.

[126] Whether or not to require compliance with the report to justice and detention scheme was also considered. As discussed above, the existing scheme of section 490 is a poor fit for seizures of intangible data. Instead, the new scheme that has been proposed above in recommendation 5.2 should also apply when police execute a warrant for overt remote access to data.

[127] Finally, it should be noted that law enforcement will continue to need the ability to *covertly* access computer systems. The Working Group acknowledges that covert access to computers can be a legitimate law enforcement tool, and covert access techniques should continue to be capable of being authorized by the general warrant provision in s. 487.01. The present proposal would supplant the use of general warrants only in respect of authorizing *overt* remote access.

Recommendation 6:

The Working Group recommends the creation of a warrant to authorize police, within a specified time period, to remotely access and copy data that are contained in or available to a computer system, without the need to enter a physical place. Preconditions for issuance should include that the applicant provide evidence of reasonable beliefs that an offence has been committed, and that data contained in or available to a computer system will afford evidence of that offence. The provision should invite the inclusion of terms that limit the scope of data that police may access and copy.

The provision should require that notice be given, where feasible, to the person having possession or control of the data thus accessed. Notice should be requires to be given forthwith or as soon as practicable after access is carried out, with an option to seek waiver of the notice obligation if a justice is satisfied that giving notice would be impracticable.

The new scheme in recommendation 5.2 for reporting and keeping data should apply to data obtained through the remote access warrant.

3.7 Correcting errors in unexecuted warrants

[128] Sometimes warrants are issued that contain a small but significant error – such as an error in an address or a date – that means they cannot validly be executed.[91] Currently, there is no statutory means to correct a 487 warrant that is discovered to contain an error after issuance but before execution. The only route available to police is to not execute the warrant, and re-apply by a fresh application.[92] Depending on local courthouse procedures and on the timing of when the error is discovered, the fresh application may or may not be able to be given to the same justice who considered the first application. Thus two judicial officials may end up doing substantially the same work, since the second judicial official is required to make their own independent decision about issuance of the second warrant.

[129] In contrast, the existing production order scheme contains a useful authority that allows police to apply to revoke or vary a production order: subsection 487.019(3) of the *Criminal Code*. On application in the prescribed form, the applicant can set out briefly that the error was noticed before execution, and describe how it should be fixed. The justice can then vary the order to fix the error, or can rescind the order. That is, instead of a judicial official potentially re-reading the entire application for the sake of a small correction, a short supplemental affidavit justifies the correction.

[130] It would benefit the administration of justice if minor clerical errors in 487 war-

---

[91] A recent example is the case of *R. v. Pampena*, 2022 ONCA 668. In that case, a police officer made a typing error by transposing two digits the address of a certain residence for which a search warrant was sought: 1105, instead of 1015, Galesway Boulevard. The error carried through into the warrant. Without noticing the error, police purported to execute the warrant at the address they *intended* to search, which was *not* the address stated on the warrant. The consequence of the error was a warrantless, illegal search.

[92] *R. v. Athwal*, 2017 ONSC 96 at paras. 130-31, 143.

rants could also be corrected through a short supplemental application supporting a variation, instead of police being required to re-apply with a new application.

Recommendation 7:

The Working Group recommends enactment of a power for a justice to vary a search warrant to correct minor drafting errors prior to execution of the warrant.

3.8 Warrants authorizing entry at night

[131] Section 488 of the *Criminal Code* requires that a 487 warrant be executed in daytime hours (defined in section 2 as being between 6:00 a.m. and 9:00 p.m.), unless the justice is satisfied on reasonable grounds and explicitly authorizes that the warrant may be executed at night. The current section reads:

> Execution of search warrant
>
> **488** A warrant issued under section 487 or 487.1 shall be executed by day, unless
>
> (a) the justice is satisfied that there are reasonable grounds for it to be executed by night;
>
> (b) the reasonable grounds are included in the information; and
>
> (c) the warrant authorizes that it be executed by night.

[132] Courts have identified a number of factors the justice should consider in applying section 488 that are not apparent from the text of the section.

[133] The jurisprudence is clear that nighttime execution of a 487 warrant to search a dwellings should only be done in exceptional circumstances.[93] In the case of *L.V.R.*, the British Columbia Court of Appeal articulated a "common sense" approach to assessing whether an objectively reasonable basis exists to authorize nighttime execution of search warrant.[94] "Necessity" to search at night is not required.[95] Instead, the issuing justice must balance the competing private and public interests, including:

---

[93] *R. v. Sutherland*, 2000 CanLII 17034 (Ont. C.A.) at paras. 21-33.

[94] *R. v. L.V.R.*, 2014 BCCA 349 at paras. 24-28.

[95] *R. v. L.V.R.*, 2014 BCCA 349 at paras. 25.

- The nature and gravity of the offences under investigation[96]
- Whether or not the place to be searched is a dwelling, and the likelihood of occupancy at the time of the search[97]
- Safety concerns including the anticipated presence of firearms at the place to be searched[98]
- The specific needs of the investigation, including any urgency or any need for police to maintain security of the premises until search[99]
- The nature of the things to be seized, including the likelihood of them being disposed of or hidden[100]

[134] These considerations are not reflected in the text of the provision. The Working Group recommends that some version of these factors be codified into the statutory test.

[135] It may be asked, why amend the section if the law as judicially interpreted already appears to function well? Members of the Working Group advanced arguments both for and against codifying the factors that arise from caselaw. The argument against legislating where courts have already spoken is that articulating the relevant factors in legislation may have the effect of "freezing" the law against future development by the courts when unanticipated situations arise. One response to this concern is that flexibility need not be lost if the list of relevant factors is written as a non-exhaustive list.

[136] The argument in favour of codifying is simply that members of law enforcement and members of the public – most of whom are not trained in conducting legal research – would be better able to know and understand the law if it were made accessible in the text of statute. And when police better know the legal test to be met, judicial officials will be provided with better relevant evidence that addresses the question to be decided

---

[96] *R. v. Peddle*, 1997 CanLII 16100 (Nfld. Sup. Ct.) at paras. 4-6; *R. v. L.V.R.*, 2014 BCCA 349 at para. 26; *R. v. Carstairs*, 2022 BCCA 69 at paras. 35-37.

[97] Search of an unoccupied dwelling is understood to be less intrusive than if a resident is present: *R. v. Brown*, 2008 ABQB 663 at para. 59; *R. v. Johnson*, 2009 MBQB 271 at para. 37; *L.V.R.*, 2014 BCCA 349 at para. 27; *R. v. Carstairs*, 2022 BCCA 69 at paras. 38-39.

[98] *R. v. Macdonald*, 2012 ONCA 244 at paras. 25-29; *R. v. Lowe*, 2018 ONCA 110 at paras. 64-67.

[99] *R. v. L.V.R.*, 2014 BCCA 349 at para. 28.

[100] *R. v. Carstairs*, 2022 BCCA 69 at paras. 40 and 43.

when an application that is brought before them.

[137] Although this recommendation is not a pressing concern, on balance the Working Group recommends codification of a non-exhaustive list of factors to be considered, similar to those articulated in the *L.V.R.* case.

[138] It should be noted, Parliament has decided that warrants issued under the *Controlled Drugs and Substances Act* are not subject to the requirements of section 488 of the *Criminal Code*.[101] Amending section 488 would not affect *CDSA* warrants. Nor would amendments affect the more recently enacted *Cannabis Act*, which contains a similar search warrant provision to the *CDSA*. Both statutes provide for execution of search warrants "at any time".[102]

Recommendation 8:

Section 488 of the *Criminal Code* should be amended to codify the non-exhaustive list of factors to be considered in deciding whether or not to authorize night entry under a search warrant.

3.9 Sealing and non-publication provisions

[139] Section 487.3 of the *Criminal Code* provides for orders prohibiting access to or disclosure of materials filed in relation to an application for a warrant, a production order, or a *Feeney* warrant. These orders are commonly referred to as sealing orders.

[140] The section outlines the bases upon which sealing may be granted, but it does not completely capture the relevant legal considerations as they have developed in the jurisprudence. In particular, the "*Dagenais/Mentuck* test," arising from a series of decisions of the Supreme Court of Canada, should be codified into section 487.3 so that the statute accurately represents the legal test that must be applied by courts. Through the cases of *Dagenais v. CBC*,[103] *R. v. Mentuck*,[104] and *Toronto Star v. Ontario*,[105] the Supreme Court of Canada has added additional considerations to the statutory factors listed

---

[101] *R. v. Saunders*, 2003 NLCA 63 at paras. 27-34; *R. v. Dueck*, 2005 BCCA 448 at paras. 17-21; *R. v. Shivrattan*, 2017 ONCA 23 at paras. 60-61.

[102] *Controlled Drugs and Substances Act* section 11, and *Cannabis Act* section 87.

[103] *Dagenais v. Canadian Broadcasting Corp.*, [1994] 3 S.C.R. 835.

[104] *R. v. Mentuck*, 2001 SCC 76.

[105] *Toronto Star Newspapers Ltd. v. Ontario*, 2005 SCC 41.

in section 487.3. The *Dagenais/Mentuck* test requires that before making any discretionary order that derogates from the constitutionally protected open courts principle[106] – including a sealing order – a court must first consider:

- The order must be necessary to prevent a serious risk to the proper administration of justice because reasonably alternative measures will not prevent the risk; and

- The salutary effects of the order must outweigh the deleterious effects on the rights and interests of the parties and the public, including the effects on the right to free expression, the right of the accused to a fair and public trial, and the efficacy of the administration of justice.

[141] These mandatory considerations are not well reflected in the provision. In particular, the requirement to consider lesser alternative measures is not readily apparent from the current text of section 487.3. The Working Group recommends that the section should be amended so that it better reflects the *Dagenais/Mentuck* test, in addition to the current statutory considerations.

[142] The same debate engaged in the preceding section of this report – why codify the common law that already works well? – can also be engaged in relation to this recommendation. However there was consensus within the Working Group that the argument for codifying the *Dagenais/Mentuck* test into section 487.3 is compelling. The open courts principle enjoys constitutional protection, under the free expression and free press rights in section 2(b) of the *Charter*. Judicially "reading in" the *Dagenais/Mentuck* considerations into section 487.3 is necessary to make the provision constitutional. It would benefit the administration of justice to ensure that the provision unambiguously reflects what the Supreme Court of Canada has said are constitutional requirements.

Recommendation 9.1:

Section 487.3 of the *Criminal Code* should be amended to codify the *Dagenais/Mentuck* test that must be applied when a court considers whether to grant a sealing order under that section.

[143] The Working Group considered two further issues around the sealing order provision. First, it is not always clear whether section 487.3 of the *Criminal Code* is capable of being applied to materials filed in applications under section 490 for continued detention of seized things.

---

[106] *Toronto Star Newspapers Ltd. v. Ontario*, 2005 SCC 41 at paras. 7, 28.

[144] One difficult scenario is when things are seized without warrant (*e.g.* incident to arrest). Section 487.3 provides that when a warrant, production order, or authorization is sought, if the prescribed conditions are met, then "information relating to the warrant, order or authorization" may be ordered sealed. But when a seizure was warrantless, there is no warrant, production order, or authorization to satisfy the threshold condition for invoking section 487.3. One court answered this problem by concluding that when continued detention was sought for things seized without warrant, a sealing order over those materials could be granted through the court's inherent authority to seal its own records.[107] (Reliance on implied or inherent authority to make a sealing order is well supported by appellate jurisprudence.[108])

[145] Second, even when there is a warranted seizure, it is not clear that materials filed on an application for continued detention, months after the warrant issued, come within the meaning of the words "information relating to the warrant, order or authorization." And more significantly, it is not clear whether the grounds for sealing that were offered at the time the warrant issued can continue to be relied upon to seal documents created months later.[109]

[146] The same questions arise when a person having an interest in the seized property seeks return of or access to the property (subsections 490(7), 490(10), 490(15)).

[147] It may be asked, what could need to be sealed in these circumstances? The answer is that in each of the circumstances outlined here, there could be good reasons why police wish to justify continued detention of the things for purposes of an ongoing investigation, or resist providing access to the things, but without revealing those reasons through publicly accessible court filings. Section 487.3 already recognizes that, in some cases, the needs to protect the identity of an informer, or the secrecy of the details an ongoing investigation or investigative technique, or to avoid prejudice to the interests of an innocent person, may exceed the public's interest in open access. Those law enforcement interests can equally arise when seeking to meet a legal test under section 490. In appropriate cases, it should be open to a court to order that materials filed in a proceeding under section 490 are sealed.

---

[107] *Application to extend seizure of exhibits and to seal affidavits*, 2007 BCPC 281.

[108] *R. v. Toronto Star Newspapers Ltd.* (2003), 67 O.R. (3d) 577 (C.A.), aff'd *sub nom. Toronto Star Newspapers Ltd. v. Ontario* 2005 SCC 41.

[109] *Further Detention of Things Seized (Re)*, 2020 BCSC 1100 at paras. 17-29.

[148] Although a court's inherent jurisdiction to control its records does provide authority to seal whatever does not come within the scope of section 487.3, the Working Group recommends that the scope of the provision should also be adjusted so that it explicitly is capable of being applied in the context of materials filed in all proceedings under section 490, whether relating to a warranted or a warrantless seizure.

Recommendation 9.2:

The scope of section 487.3 of the *Criminal Code* should be adjusted so that it clearly is capable of being applied in the context of materials filed in all proceedings under section 490, whether relating to a warranted or warrantless seizure.

[149] Second, there is a strange procedural challenge around the reviewability of orders made under section 487.3. Any party affected by the order can apply to terminate or vary the order, pursuant to subsection 487.3(4). However no statutory path to an appeal court is provided following that application, with the result that appeal rights are wildly different depending on whether the order was made in provincial court, or in superior court. This should be changed.

[150] The case of *Mentuck*, referred to already, was an unusual appeal that proceeded directly from the court of first instance, the Manitoba Court of Queen's Bench, to the Supreme Court of Canada by way of leave granted under section 40 of the *Supreme Court Act*, without first passing through the Manitoba Court of Appeal. This direct route of appeal is considered by the Supreme Court to be undesirable, and it is permitted only as a last resort because third parties who are affected by an order that derogates from the open courts principle sometimes have no other legal recourse to seek review of the order. The Court expressed its view that legislative change is needed:

> I would here reiterate Lamer C.J.'s observation [in *Dagenais*[110]] that the current situation, which fails to provide satisfactory routes of appeal despite the fundamental rights at stake, is "deplorable", and again express the hope that Parliament will soon fill this unnecessary and troublesome gap in the law. In that respect, I should like to emphasize that our Court and our judicial system generally greatly benefit from the role of the courts of appeal, and to eliminate their input on these important questions is most regrettable.[111]

---

[110] *Dagenais v. CBC*, [1994] 3 S.C.R. 835 at 874.

[111] *R. v. Mentuck*, 2001 SCC 76 at para. 17.

While the *Mentuck* case was not itself about a section 487.3 order, the complaint about appeal procedure is equally relevant here.

[151] The procedural options currently available to seek review of an order made under section 487.3 are arcane. First, as noted, anybody can apply under subsection 487.3(4) to terminate or vary the order.[112] That application is heard in the court that granted the initial order. But, absent any statutory path to an appellate court, litigants who wish to appeal the outcome are left to resort to one of two residual sources of authority. Where the order was made in an inferior court (such as a provincial criminal court), an application for judicial review by way of *certiorari* can be made to a superior court. *Certiorari* is available only for review of decisions made by inferior courts; *certiorari* cannot be used to review an order that was itself made by a superior court.[113] Thus in a case where the section 487.3 order was made by a superior court, the only review available after an application under subsection 487.3(4) is an application for leave to appeal directly to the Supreme Court of Canada. This leads to the unfortunate and arbitrary result that some orders are reviewable locally by way of *certiorari*, and the outcome of that review can be appealed to the provincial court of appeal via section 784 of the *Criminal Code*, while other orders are not reviewable beyond the subsection 487.3(4) procedure, except by a direct appeal, by leave, to the Supreme Court of Canada. It is the latter scenario that was noted by the Supreme Court of Canada in *Dagenais* and again in *Mentuck* to be "deplorable."

[152] When Parliament revisits section 487.3, it should consider providing a statutory path by which a third party who is directly affected by an order made under section 487.3, and who has no other legal recourse to challenge the order, can apply for leave to appeal to a provincial court of appeal. Given the general undesirability of interlocutory appeals in criminal matters,[114] this new path should be available only in relation to an order that has already been subject to an application to vary under subsection 487.3(4), and that has a "final and conclusive" affect on the rights of the third party.

---

[112] There is no restriction on who can make an application under subsection 487.3(4) of the *Criminal Code*. Consequently it can be made by a suspect or accused person, by the police, by the prosecutor, or by any member of the public. These applications are often made by members of the press.

[113] *R. v. Awashish*, 2018 SCC 45 at paras. 19.

[114] *R. v. Awashish*, 2018 SCC 45 at paras. 11-20.

Recommendation 9.3:

The Working Group recommends that an appeal to the provincial court of appeal be available, by leave of the court of appeal, after a decision is made pursuant to subsection 487.3(4) of the *Criminal Code* as to the application by a third party for termination or variation of an order made under section 487.3.

[153] Finally, the Working Group considered section 487.2 of the *Criminal Code*. That section purports to prohibit publication of information about the location of a place to be searched, the identity of an occupant of that place, and the identity of a person suspected to be involved in an offence, unless a charge has been laid in respect of an offence that is identified in the search warrant. The section appears to have been well motivated toward protecting the reputational interests of innocent persons who are subjected to searches by police. However, that motivation is clearly in conflict with the *Charter*-protected rights of freedom of the press, and consequently the section has been declared of no force or effect in at least three provinces, for violating section 2(b) of the *Charter*.[115] It appears that the Federal government believes it to be inoperative.[116] The Working Group recommends that Parliament should repeal the section.

Recommendation 9.4:

Section 487.2 of the *Criminal Code* should be repealed.

[115] *Canadian Newspapers Co. Ltd. v. Canada (A.G.)* (1986), 55 O.R. (2d) 737 (H.C.); *Canadian Newspapers Co. Ltd. v. Canada (A.G.)*, 1986 CanLII 3911 (Man. Q.B.); *Girard c. Demers*, 2001 CanLII 9809 and 2001 CanLII 39738 (Que. C.A).

[116] According to the Québec Court of Appeal, the section was "described as 'inoperative' by the Federal Minister of Justice" shortly after the 1986 declarations in Ontario and Manitoba, and the Attorney General of Canada did not appear to defend the constitutional challenge in Québec: *Girard c. Demers*, 2001 CanLII 39738 (Que. C.A) at paras. 6-8.

4. SUMMARY OF RECOMMENDATIONS

Recommendation 1.1:

The Working Group recommends that the words "suspected to have been committed" be removed from section 487 of the *Criminal Code*.

Recommendation 1.2:

The Working Group recommends that paragraphs 487(1)(a), (b), and (c) of the *Criminal Code* be combined into a single paragraph that is focused on seizing things that will afford evidence of an offence, based on the legal standard of reasonable belief and without reference to suspected offences. The function of current paragraph 487(1)(c.1), that is, providing authority for seizure of offence-related property, should be maintained.

Recommendation 1.3:

The Working Group recommends that the terms "building" and "receptacle" be deleted throughout section 487 of the *Criminal Code*, leaving only the word "place." A new definition of "place" should be added, stating that a place includes a building, receptacle, or conveyance. Confusing references in Form 1 and Form 5 to "premises" and "dwelling-houses" should be removed.

Recommendation 1.4:

The Working Group recommends that Parliament should consider whether section 487 of the *Criminal Code* should be amended to explicitly allow that the issuing justice may include terms and conditions that the justice considers appropriate to ensure the warrant is reasonable.

Recommendation 2:

The Working Group recommends that the confusing state of law about vehicles within curtilage should be clarified. This could be accomplished if the definition of "dwelling-house" is amended, or a definition of "place" is added, in relation to search warrants only, to clarify whether or not a dwelling-house (or building) includes a motor vehicle (or conveyance) located within the curtilage but outside the building or connected structures.

Recommendation 3:

The Working Group recommends that section 487 of the *Criminal Code* be amended to add a provision analogous to subsection 11(5) of the *Controlled Drugs and Substances Act* and subsection 87(5) of the *Cannabis Act*, to clearly allow for searches of persons found at the place to be searched, when an officer has reasonable grounds to believe they have on their person one of the things authorized to be seized under the search warrant.

Recommendation 4.1:

The Working Group recommends that the nature of the entry and search capable of being authorized by a *Criminal Code* 487 warrant be expanded, to allow for police to enter a place in order to make observations of the place and of things found therein that there are reasonable grounds to believe will afford evidence of an offence, and to document those observations, including by way of photographs, video recordings, and other measurements, without a precondition that police search for and seize any tangible thing. The amendment should indicate that the existing authority of police to document the execution of a warranted search is not affected.

Recommendation 4.2:

The Working Group recommends that the enter-to-observe authority in recommendation 4.1 should provide that officers may enter and observe by accessing the place remotely, by means of telecommunication. Entry and observation by means of telecommunication should include a mandatory condition of execution that police announce the entry, to ensure the observations are conducted overtly.

Recommendation 5.1:

The Working Group recommends the creation of a new form of warrant for a specified examination or analysis of computers and computer data. The purpose or scope of examination or analysis should be prescribed in the terms of the warrant. The warrant should be available either in conjunction with a *Criminal Code* 487 warrant or separately. Preconditions for issuance should include that the applicant reasonably believes an offence has been committed, and that the proposed examination or analysis will afford evidence of that offence.

Notice should be given of the examination warrant. When the examination warrant is joined with a *Criminal Code* 487 search and seizure warrant, notice is achieved by means of the Form 5.1 that is required to be given under section 487.093 of the *Criminal Code*; that notice will indicate police have an examination warrant and thus that police intend to access data from the device. However when the examination warrant is obtained after the physical seizure, written notice of the examination warrant should be required to be sent to (a) the person from whom the device was seized, if known, and (b) a person who has asserted an interest in receiving notice about examination of the data, if any, or (c) if there is no person under either of the previous categories, then by delivering the notice to the address of the place from which the device was seized if feasible to do so. Waiver of the notice obligation should be capable of being granted by a Justice of the Peace if police show it is not practicable to give notice, or if sufficient notice has already been given.

Recommendation 5.2:

The Working Group recommends amending the *Criminal Code* so that when a warrant for the examination or analysis of data is executed, a report must be made to a justice in regard to the seizure of data. Data that is *within* the scope of the warrant should then be allowed to be kept and used by law enforcement.

Any data *outside* the scope of the warrant that was required to be seized should also be kept, for an initial period of one year, renewable, or for so long as necessary after proceedings are instituted. However, this out-of-scope data set should be destroyed within a defined period after the end of the proceedings (with allowance provided for appeal periods), or after a decision is made not to lay charges, unless police first obtain a new order for continued possession of the data.

A mechanism to allow an interested person to access seized data should be provided. Any person with a legal interest in the data should be able to request access if they can demonstrate that access is necessary to advance that legal interest. Access or provision of a copy of data should be subject to any conditions that might be imposed by the court.

Finally, copies of the data should be deemed to have the same evidential value as the data seized if they can be certified as true copies of the data seized by the person who made them or if their conformity can be demonstrated by other means.

Recommendation 6:

The Working Group recommends the creation of a warrant to authorize police, within a specified time period, to remotely access and copy data that are contained in or available to a computer system, without the need to enter a physical place. Preconditions for issuance should include that the applicant provide evidence of reasonable beliefs that an offence has been committed, and that data contained in or available to a computer system will afford evidence of that offence. The provision should invite the inclusion of terms that limit the scope of data that police may access and copy.

The provision should require that notice be given, where feasible, to the person having possession or control of the data thus accessed. Notice should be requires to be given forthwith or as soon as practicable after access is carried out, with an option to seek waiver of the notice obligation if a justice is satisfied that giving notice would be impracticable.

The new scheme in recommendation 5.2 for reporting and keeping data should apply to data obtained through the remote access warrant.

Recommendation 7:

The Working Group recommends enactment of a power for a justice to vary a search warrant to correct minor drafting errors prior to execution of the warrant.

Recommendation 8:

Section 488 of the *Criminal Code* should be amended to codify the non-exhaustive list of factors to be considered in deciding whether or not to authorize night entry under a search warrant.

Recommendation 9.1:

Section 487.3 of the *Criminal Code* should be amended to codify the *Dagenais/Mentuck* test that must be applied when a court considers whether to grant a sealing order under that section.

Recommendation 9.2:

The scope of section 487.3 of the *Criminal Code* should be adjusted so that it clearly is capable of being applied in the context of materials filed in all proceedings under section 490, whether relating to a warranted or warrantless seizure.

Recommendation 9.3:

The Working Group recommends that an appeal to the provincial court of appeal be available, by leave of the court of appeal, after a decision is made pursuant to subsection 487.3(4) of the *Criminal Code* as to the application by a third party for termination or variation of an order made under section 487.3.

Recommendation 9.4:

Section 487.2 of the *Criminal Code* should be repealed.

APPENDIX: SECTION 487 AND FORM 5 OF THE CRIMINAL CODE

(as of the latest amendments by 2019, c. 25, s. 191)

Information for search warrant

487 (1) A justice who is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that there is in a building, receptacle or place

(a) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed,

(b) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,

(c) anything that there are reasonable grounds to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant, or

(c.1) any offence-related property,

may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial

Dénonciation pour mandat de perquisition

487 (1) Un juge de paix qui est convaincu, à la suite d'une dénonciation faite sous serment selon la formule 1, qu'il existe des motifs raisonnables de croire que, dans un bâtiment, contenant ou lieu, se trouve, selon le cas :

a) une chose à l'égard de laquelle une infraction à la présente loi, ou à toute autre loi fédérale, a été commise ou est présumée avoir été commise;

b) une chose dont on a des motifs raisonnables de croire qu'elle fournira une preuve touchant la commission d'une infraction ou révélera l'endroit où se trouve la personne qui est présumée avoir commis une infraction à la présente loi, ou à toute autre loi fédérale;

c) une chose dont on a des motifs raisonnables de croire qu'elle est destinée à servir aux fins de la perpétration d'une infraction contre la personne, pour laquelle un individu peut être arrêté sans mandat;

c.1) un bien infractionnel,

peut à tout moment décerner un mandat autorisant un agent de la paix ou, dans le cas d'un fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé

law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant

notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé :

(d) to search the building, receptacle or place for any such thing and to seize it, and

d) d'une part, à faire une perquisition dans ce bâtiment, contenant ou lieu, pour rechercher cette chose et la saisir;

(e) subject to any other Act of Parliament, to, as soon as practicable, bring the thing seized before, or make a report in respect thereof to, the justice or some other justice for the same territorial division in accordance with section 489.1.

e) d'autre part, sous réserve de toute autre loi fédérale, dans les plus brefs délais possible, à transporter la chose devant le juge de paix ou un autre juge de paix de la même circonscription territoriale ou en faire rapport, en conformité avec l'article 489.1.

Execution in Canada
(2) A warrant issued under subsection (1) may be executed at any place in Canada. A public officer named in the warrant, or any peace officer, who executes the warrant must have authority to act in that capacity in the place where the warrant is executed.

Exécution au Canada
(2) Le mandat peut être exécuté en tout lieu au Canada. Le fonctionnaire public qui y est nommé ou tout agent de la paix qui exécute le mandat doit être habilité à agir à ce titre dans le lieu où celui-ci est exécuté.

Operation of computer system and copying equipment
(2.1) A person authorized under this section to search a computer system in a building or place for data may

Usage d'un système informatique
(2.1) La personne autorisée à perquisitionner des données contenues dans un ordinateur se trouvant dans un lieu ou un bâtiment peut :

(a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;

a) utiliser ou faire utiliser tout ordinateur s'y trouvant pour vérifier les données que celui-ci contient ou auxquelles il donne accès;

(b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

b) reproduire ou faire reproduire des données sous forme d'imprimé ou toute autre forme intelligible;

(c) seize the print-out or other

c) saisir tout imprimé ou sortie de

output for examination or copying; and

(d) use or cause to be used any copying equipment at the place to make copies of the data.

données pour examen ou reproduction;

d) utiliser ou faire utiliser le matériel s'y trouvant pour reproduire des données.

Duty of person in possession or control
(2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

(a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for;

(b) to obtain a hard copy of the data and to seize it; and

(c) to use or cause to be used any copying equipment at the place to make copies of the data.

Obligation du responsable du lieu
(2.2) Sur présentation du mandat, le responsable du lieu qui fait l'objet de la perquisition doit faire en sorte que la personne qui procède à celle-ci puisse procéder aux opérations mentionnées au paragraphe (2.1).

Form
(3) A search warrant issued under this section may be in the form set out as Form 5 in Part XXVIII, varied to suit the case.

Formule
(3) Un mandat de perquisition décerné en vertu du présent article peut être rédigé selon la formule 5 de la partie XXVIII, ajustée selon les circonstances.

(4) [Repealed, 2019, c. 25, s. 191]

(4) [Abrogé, 2019, ch. 25, art. 191]

FORM 5
Warrant To Search

Canada,
Province of ___,
(territorial division).

To the peace officers in the said (territorial division) or to the (named public officers):

Whereas it appears on the oath of A.B., of ___ that there are reasonable grounds for believing that (describe things to be searched for and offence in respect of which search is to be made) are in ___ at ___, hereinafter called the premises;

This is, therefore, to authorize and require you between the hours of (as the justice may direct) to enter into the said premises and to search for the said things and to bring them before me or some other justice.

Dated this ___ day of ___ A.D. ___, at ___.

A Justice of the Peace in and for ___.

FORMULE 5
Mandat de perquisition

Canada,
Province de ___,
(circonscription territoriale).

Aux agents de la paix de (circonscription territoriale) et à (noms des fonctionnaires publics) :

Attendu qu'il appert de la déposition sous serment de A.B., de ___, qu'il existe des motifs raisonnables de croire que (décrire les choses à rechercher et l'infraction au sujet de laquelle la perquisition doit être faite) se trouvent dans ___, à ___, ci-après appelé les lieux;

À ces causes, les présentes ont pour objet de vous autoriser et obliger à entrer, entre les heures de (selon que le juge de paix l'indique), dans les lieux et de rechercher ces choses et de les apporter devant moi ou devant tout autre juge de paix.

Fait le ___jour de ___en l'an de grâce ___, à ___.

Juge de paix dans et pour ___.