
CANADA / JUDGMENT

R. v. Van Humbeck

2019 BCSC 1590

COURT

Supreme Court of British Columbia

DECIDED

19 September 2019

Source: bccourts.ca · Research copy typeset by Esheria. Not court-issued or certified.

2019 BCSC 1590 R. v. Van Humbeck

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:

R. v. Van Humbeck,

2019 BCSC 1590

Date: 20190919

Docket: 23932

Registry: Salmon Arm

Regina

v.

Nicholas Van Humbeck

Before: The Honourable Mr. Justice Gomery

Ruling on Voir Dire

Counsel for the Crown:

D. Heighes

Counsel for the Accused:

G. Verdurmen

D. Verdurmen, Articled Student

Place and Dates of Hearing:

Salmon Arm, B.C.

August 27 and 28, 2019

Place and Date of Judgment:

Salmon Arm, B.C.

September 19, 2019

Introduction

- [1] Mr. Van Humbeck is charged with possession and distribution of child pornography. He applies for a ruling that electronic devices were improperly seized from his home and searched pursuant to two warrants issued by a provincial court judge on April 18, 2018 and May 28, 2018. Mr. Van Humbeck says that this was an unreasonable search and seizure that violated his rights under s. 8 of the Canadian Charter of Rights and Freedoms [Charter]. He seeks exclusion of evidence obtained under the warrants pursuant to s. 24(2) of the Charter.
- [2] I am told that Mr. Van Humbeck was arrested and charged when the first warrant was executed at his home on April 19, 2018. He also seeks a ruling that the arrest violated his right not to be arbitrarily detained or imprisoned under s. 9 of the Charter.
- [3] The only evidence on this voir dire hearing is a binder containing the two warrants in issue and the two informations to obtain ("ITOs") sworn by a peace officer, Constable St-Armand, to obtain them. I have not heard testimonial evidence from Constable St-Armand. The second ITO states that the first warrant was executed at Mr. Van Humbeck's residence and several computers, hard drives, thumb drives, an iPad and DVDs were seized. I have no other evidence as to what has taken place under the warrants and do not know how the search was conducted at the residence. It is common ground that a Crown witness or witnesses later analyzed storage media seized under the warrants and extracted images that the Crown wishes to adduce in evidence. The ruling sought by Mr. Van Humbeck would prevent that.
- [4] As it was developed in oral submissions by Mr. Van Humbeck's counsel, Mr. Verdurmen, there are three parts to the challenge presented on the voir dire:
1. The ITO sworn to obtain the first warrant is deficient on its face and fails to present reasonable and probable grounds for issuance of a warrant to search electronic storage media;
 2. On its face, the first warrant does not authorize a search of electronic devices and storage media; and
 3. The ITO sworn to obtain the second warrant and the second warrant are tainted by the unconstitutionality of the search and seizure under the first warrant.

- [5] The record is sufficient to address these arguments. It is not sufficient to enable me to assess whether Mr. Van Humbeck was arbitrarily detained on April 19, 2018 because I have not heard from the arresting officer and do not know on what basis he made the arrest.

Legal framework

- [6] Section 487 of the Criminal Code, R.S.C., 1985, c. C-46 requires a justice issuing a warrant to be satisfied by information on oath that there are reasonable grounds to believe there is in a building, receptacle or place anything that there are reasonable grounds to believe "will afford evidence with respect to the commission of an offence". The standard is one of reasonable probability or reasonable belief. Reasonable grounds are said to exist at the point at which credibly-based probability replaces suspicion; *R. v. Le* (sub nom *R. v. Liu*), 2014 BCCA 166 [Le] at para. 39.
- [7] This *voir dire* requires that I review the decisions to issue the warrants applying the test first enunciated in *R. v. Garofoli*, [1990] 2 S.C.R. 1421 at 1452. The warrants are presumptively valid. My role is not to determine whether I would issue either warrant on the basis of the ITO presented to the judge, but rather to consider whether the material could support the issuance of the warrant; *R. v. Wilson*, 2011 BCCA 252 at paras. 37 and 63. I am to examine the information in its totality, not piecemeal, on a "practical, non-technical and common-sense basis"; *Le* at para. 39.
- [8] All searches potentially engage the constitutional protection against unreasonable search and seizure under s. 8 of the Charter because the state's interest in investigating criminal activity runs up against the individual's right to be let alone. Searches of electronic storage media present special challenges because of the potential range and depth of the intrusion into personal and private affairs. As Cromwell J. observed in *R. v. Fearon*, 2014 SCC 77 at para. 197:

... It is difficult to conceive of a sphere of privacy more intensely personal - or indeed more pervasive - than that found in an individual's personal digital device or computer.

- [9] The cases recognize these challenges by imposing safeguards. Where electronic devices are concerned, the usual rule that authority to search a place affords authority to search receptacles in that place, is abandoned. Express authority to search electronic storage media must be set out in a warrant; *R. v. Vu*, 2013 SCC 60 [Vu] at paras. 45-49. The warrant must be obtained before electronic storage media are searched. The purpose of this requirement is to give the justice issuing the warrant an opportunity to assess the privacy interests at play and specifically consider whether there are reasonable grounds for a search in the circumstances.

[10] An ITO to obtain a warrant must demonstrate rather than simply asserting the existence of reasonable grounds. The justice issuing the warrant must be afforded an opportunity to make an objective assessment of the grounds relied upon. In *R. v. Morelli*, 2010 SCC 8 [Morelli], there was an issue as to whether an ITO provided reasonable grounds for a search of the accused's electronic devices for child pornography. At para. 62, Fish J., speaking for the majority, said that the issue depended on:

whether the ITO, stripped of its erroneous and tendentious assertions, and amplified as indicated, provides sufficient credible and reliable evidence to have permitted the justice of the peace to find reasonable and probable grounds to believe both that the appellant was in culpable possession of child pornography and that evidence of that crime would be found in his computer.

[11] In *Morelli*, the evidence was lacking. Fish J. cautioned against reliance on unsubstantiated statements in the ITO concerning the propensities of certain types of offenders.

[12] The requirement for express preauthorization of a forensic search of electronic storage media does not generally entail that a search warrant must set out a protocol for the conduct of the forensic search; *Vu* at paras. 54-59. At para. 61, Cromwell J. added:

[61] By now it should be clear that my finding that a search protocol was not constitutionally required in this case does not mean that once police had the warrant in hand, they had a licence to scour the devices indiscriminately. They were bound, in their search, to adhere to the rule that the manner of the search must be reasonable. Thus, if, in the course of their search, the officers realized that there was in fact no reason to search a particular program or file on the device, the law of search and seizure would require them not to do so.

[13] Any issue of the reasonableness of the forensic search of electronic devices seized in this case has not been addressed on this *voir dire*.

Analysis

1. Was it open to the judge to conclude that the ITO sworn to obtain the first warrant presented reasonable and probable grounds for issuance of a warrant to search electronic storage media?

[14] The first ITO may be summarized as follows.

[15] Constable St-Amand swore that an investigation began in June 2017 with a report to Salmon Arm RCMP through law enforcement intermediaries originating with Yahoo! Inc. ("Yahoo"). Yahoo reported that a user based in Canada had uploaded one image of suspected child pornography on September 22, 2016 and two images on June 5, 2017. Yahoo identified the user by a 26 character alphanumeric code associated with an account in Mr. Van Humbeck's name and provided a telephone number, two email addresses, and an IP address.

- [16] The images were reviewed by another constable who provided to Constable St-Amand a detailed description furnishing reasonable and probable grounds for a characterization of them as child pornography as it is defined in s. 163.1(1)(a) of the Criminal Code.
- [17] The other constable obtained a production order directed to Shaw Communications. The order sought the subscriber name, address and telephone number associated with an IP address. There is a one-digit discrepancy between the IP address associated with the production order and the IP address reported as having been received from Yahoo. Crown Counsel attributed the discrepancy to a typographical error in the ITO. Shaw Communications reported that the IP address was associated with a residential customer account in Mr. Van Humbeck's name with the telephone number and one of the email addresses reported by Yahoo. Apart from the IP address, this evidence connects the information provided by Shaw Communications to the earlier Yahoo report. Shaw Communications also provided a residential address. Its accounts were paid from a bank account in Mr. Van Humbeck's name.
- [18] Constable St-Amand conducted searches confirming that Mr. Van Humbeck has a current driver's licence listing him as resident at the address reported by Shaw Communications, and that he owns a vehicle with the vehicle registration reporting the same address. The other constable drove by the residence and observed Mr. Van Humbeck's vehicle parked outside with fresh tracks in the snow, and another vehicle registered to a second person apparently living at the same address. Mr. Van Humbeck was observed entering the residence. Further inquiries identified Mr. Van Humbeck's employer and a Facebook profile page apparently maintained by Mr. Van Humbeck.
- [19] The first ITO was sworn on April 18, 2018. Constable St-Amand identified Mr. Van Humbeck as a person believed guilty of possessing, distributing and making available child pornography between September 21, 2016 and June 6, 2017. He stated that he believed that Mr. Van Humbeck was still in possession of child pornography on computer devices at his home. He identified himself as a person having extensive experience with computers and stated that he was aware that computer users often amass large quantities of data such as image files and retain them for many years. He said that even when files are deleted, they can often be recovered through a forensic examination.
- [20] Constable St-Amand sought a warrant to search Mr. Van Humbeck's residence and seize electronic devices. The ITO contemplates a forensic search of electronic storage media on the devices.
- [21] Mr. Verdurmen submits that the ITO provides grounds for suspicion but not reasonable grounds for belief. He emphasizes the following points:
- a) Only three images of child pornography were identified. Mr. Verdurmen describes these as isolated instances;

- b) The investigation conducted subsequent to receipt of the report from Yahoo was superficial and did not turn up inculpatory evidence;
 - c) The evidence of uploading of images was stale. One was uploaded 19 months before the ITO was sworn, and the other two were uploaded 10 months before the ITO was sworn;
 - d) The IP address identified in the ITO was tied to a particular residence, but not to any particular device. Many devices are mobile. Mr. Verdurmen suggests that it is no more than speculation to think that the particular device associated with the uploading would be present in the residence during a search conducted many months later;
 - e) The ITO contains various assertions as to the propensity of "people who collect child pornography", such as an alleged propensity to collect and store images for long period of time. Mr. Verdurmen submits that this is the very reasoning that was disparaged by the Supreme Court of Canada in *Morelli*;
 - f) Unlike drugs and guns, computers and cell phones are not naturally connected or associated with criminal conduct, and a search of them involves a massive intrusion into the personal life of the user. Mr. Verdurmen argues that better evidence is required than was provided to justify such a search in this case.
- [22] I am not persuaded by these arguments that the judge lacked reasonable and probable grounds to issue a warrant to search electronic storage media at Mr. Van Humbeck's residence.
- [23] It is clear that the ITO provided reasonable and probable grounds for a belief that Mr. Van Humbeck uploaded and was in possession of an image of child pornography on September 21, 2016 and two further images on June 6, 2017. These would be two distinct episodes of the criminal offence under s. 163.1(4) of the Criminal Code. The fact that the investigating officers had no evidence of further episodes does not detract from the evidence they had.
- [24] The Yahoo report indicated that the user had uploaded and not merely accessed the child pornography. The difference between uploading and accessing is that the uploading user retains the image on his or her device. Uploading implies a decision to retain, if only for a short time. The image may be deleted or discarded afterwards, but that requires further action on the part of the user. As a matter of common sense, it was open to the judge to infer that uploaded images are more likely than not to be retained for some time.
- [25] By the time the ITO was sworn, the two uploading episodes had taken place 10 and 19 months in the past. While there are all kinds of reasons the user may have decided to delete them, it was open to the judge to infer that it was more probable than not that they were still retained. In this regard, the circumstances contrast sharply with *Morelli*, where it was known that the accused had reformatted his hard drive, presumptively deleting the data saved on it, four months before the warrant was authorized.

- [26] While it is possible that the images may have been saved onto a mobile device that would not be present in Mr. Humbeck's residence when the search warrant was executed, it was open to the judge to infer that it was more likely than not that Mr. Van Humbeck would keep electronic storage media containing pornographic material in the privacy of his home.
- [27] I agree with Mr. Verdurmen that the ITO contains assertions concerning the propensities of people who collect child pornography that could not be relied upon as furnishing reasonable and probable grounds. One would hope that the RCMP's legal advisors would forestall the inclusion of statements of this kind in an ITO. However, I do not think it was necessary for the judge to rely on any of this material in concluding that a warrant should issue.
- [28] Taking the ITO in its totality but disregarding unsupported allegations of general propensity, I am satisfied that it was open to the judge to conclude that credibly based probability replaced suspicion that electronic storage media at Mr. Van Humbeck's home would furnish evidence that he was in possession of child pornography between September 21, 2016 and June 6, 2017. The ITO afforded the judge an opportunity to consider the privacy interests engaged by the request for a search warrant. Giving full weight to Mr. Van Humbeck's interest in maintaining the privacy of his personal digital records, it was open to the judge to conclude that a search of electronic storage media was justified.
2. Does the first warrant authorize a search of electronic devices and storage media?
- [29] The first warrant is attached as Appendix A to these reasons.
- [30] The warrant contains two mistakes. It states that it was issued on the oath of Constable Mikelsen, when the ITO was sworn by Constable St-Amand. And it is misdated March 18, 2018, though it was issued on April 18, 2018. Mr. Verdurmen did not contend that these mistakes were fatal, though he pointed to them as evidence of sloppy work on the part of the RCMP. Neither mistake would confuse or mislead an executing officer or a person presented with the warrant during a search as to what was authorized. These mistakes are not relevant to what I have to decide.
- [31] The warrant states that there are reasonable grounds to believe that the criminal offences of possessing, distributing and making available child pornography have been committed. It does not identify the time period under investigation.
- [32] Mr. Verdurmen submits that the warrant only authorizes a search for electronic devices, not a search of electronic devices. He points to the wording of Appendix A. Paragraph 1 begins by referring to:

All electronic processing and storage devices capable of analyzing, creating, displaying, converting, storing or transmitting electronic or magnetic computer impulses or data for:

[Emphasis added]

There follows a list of three different categories of electronic files or data:

- pornographic images or videos;
- computer files "that may assist in identifying the user of IP address 24.7.127 at the time the offence was committed"; and
- data affording evidence of access or control of the premises at the residence.

[33] Mr. Verdurmen argues that all that is authorized is a search of electronic processing and storage devices having the capability of processing the categories of data listed. On this reasoning, the warrant does not authorize a forensic search of the files themselves.

[34] Similarly, paragraph 3 refers to:

Storage media that could contain any of the above items including floppy diskettes, fixed hard disks, removable hard disks, CDs, DVDs and any other media which is capable of storing magnetic coding.

[Emphasis added]

[35] Paragraph 4 refers to:

Cellphones and tablets or any mobile devices capable of connecting to the internet for:

[Emphasis added]

There follows another list of categories of files or data.

[36] Mr. Verdurmen argues that, like paragraph 1, paragraphs 3 and 4 only authorize a search for storage media (under paragraph 3) and mobile devices (under paragraph 4) and not a search of them.

[37] Mr. Verdurmen argues that, if the warrant is ambiguous, the ambiguity must be resolved in favour of the accused, for the protection of his right to be secure against unreasonable search and seizure. At best, he maintains, this warrant is garbled and unclear and does not satisfy the requirement that a warrant authorizing a search of electronic storage media must be express, clear and unambiguous.

[38] I agree with Mr. Verdurmen that the requirement that the warrant expressly authorize a search of electronic storage media carries with it the corollary that the expression must be clear and unambiguous. A person presented with the warrant should be able to discern, without undue difficulty, what the police are authorized to search for. The warrant must be construed from the perspective of a person to whom it may be presented, and not from the perspective of the issuing justice, who also has access to the ITO; *R v. Ting*, 2016 ONCA 57 at para. 59; *R. v. Salehi*, 2019 BCSC 125 [Salehi] at paras. 37-39.

[39] Reading the warrant as a whole, I agree with Mr. Verdurmen that it is not well drafted, but I do not think it is ambiguous as to an intention to authorize a search of electronic storage media for images of child pornography. There is an ambiguity to one aspect of the warrant and I will address this matter below.

[40] While the argument focused on Appendix A, it is important to begin with the body of the warrant. After referring to the offences it is believed have been committed, it continues:

AND THAT there are reasonable grounds for believing that the following items will afford evidence of the Offences:

a. See Appendix "A"

AND THAT there are reasonable grounds for believing that the said items or some part of them are in the residence located at 11-5080 20th Avenue NE, Salmon Arm, BC.

THIS IS THEREFORE, to authorize and require you to enter the said premises between the hours of 07:00 am on the 19th day of April, 2018 to 7:00 pm on the 19th day of April, 2018, and to search for the things and to bring them before me or some other justice, or submit a report in writing in respect of anything seized.

[Emphasis added.]

[41] By these words, the warrant authorizes the holder of the warrant to enter into the identified premises and search for "things" also described as "items". The items are identified in Appendix A.

[42] Appendix A is headed, "THINGS TO BE SEARCHED FOR".

[43] I have already described and quoted parts of paragraphs 1, 3 and 4. They list both electronic devices and storage media, on the one hand, and electronic files and data, on the other. Paragraph 3 directly and unambiguously describes the electronic files listed in paragraph 1 as "items". Electronic devices cannot be "items" because electronic devices cannot be contained on storage media as paragraph 3 requires.

[44] The warrant cannot be interpreted coherently as authorizing a search for electronic devices having certain capabilities. That would require the reference to "items" in the body of the warrant to carry a different meaning than the reference to "items" in paragraph 3.

[45] Moreover, consistently with paragraph 3, paragraphs 1 and 4 each take this form:
[Description of electronic devices and storage media] for [description of electronic files or data]. The electronic files or data are the things to be searched for, and the electronic devices and storage media are the places to be searched.

[46] I should add that this is the interpretation that first comes to mind on a quick reading of the warrant. This warrant is very different from the warrant in Salehi which simply referred to "computers and electronic devices capable of accessing the internet" without any description of the object of an electronic search. Faced with this warrant, very few readers

would quickly perceive any possibility that the various categories of files and data set out are surplusage and conclude that the warrant only authorizes a search for electronic devices and storage media. The interpretation advocated by Mr. Verdumen requires a strained and attentive reading, and it is one that ultimately collapses on reflection.

[47] To summarize, on its proper interpretation, the warrant expressly, clearly and unambiguously authorizes a search of electronic devices and storage media for itemized categories of electronic files and data.

[48] However, there is an ambiguity in item 1.b. of Appendix A. It lists the following as an item to be searched for:

Computer files or documents including address and phone books, portfolios, electronic mail, chat logs, video, internet history or computerized files that may assist in identifying the user of IP address 24.7.127 at the time the offence was committed.

[Emphasis added]

[49] The reference to the time that the offence was committed is unclear because the warrant does not identify a relevant time. The IP address is incomplete and the portion that is provided is incorrect. In my opinion, these deficiencies prevent paragraph 1.b. of the Appendix from being given effect as an express authorization of a forensic search of an electronic device seized under the warrant. To the extent that anything was seized under the putative authority of paragraph 1.b., the search was unreasonable.

[50] I do not know whether anything was seized under the putative authority of paragraph 1.b. of the Appendix and am not in a position, on the record, to assess whether anything that was seized would have to be excluded from evidence pursuant to s. 24(1) of the Charter. If necessary, these are matters to be addressed on a further voir dire.

Conclusion

[51] I have held that the first warrant was properly authorized and issued, with the exception of paragraph 1.b. of the Appendix. It follows that the attack on the second ITO and warrant as tainted by the deficiencies of the first must fail.

[52] Accordingly, I decline to rule that electronic files and data extracted under the first and second warrants, other than files and data seized under paragraph 1.b. of the warrants, are inadmissible on the basis that the warrants authorized an unreasonable search and seizure contrary to s. 8 of the Charter. If files and data were seized under paragraph 1.b. of the warrants, they were not lawfully seized and it is open to the defence to argue that they should be excluded from evidence on that basis.

"Gomery J."

The Honourable Mr. Justice Gomery

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/sc/19/15/2019BCSC1590.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/r-v-van-humbeck-2019>

Prepared on 28 October 2026 · Esheria