

CANADA / JUDGMENT

R. v. Wiwchar

2024 BCSC 2442

COURT

Supreme Court of British Columbia

DECIDED

27 November 2024

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

2024 BCSC 2442 R. v. Wiwchar

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:

R. v. Wiwchar,

2024 BCSC 2442

Date: 20241127

Docket: 27393-2; 27393-215

Registry: Vancouver

Rex

v.

Dean Michael Wiwchar

Restriction on Publication: Pursuant to 486.31(1), 486.5(1), 631(6) & 648 C.C.C.

Inherent Jurisdiction

Before: The Honourable Justice Ker

Oral Ruling on Voir Dire #4 re: Crown Motion for Summary Dismissal of Application No. 215

Counsel for the Crown:

M.J. Sheardown

S.L. Dworkin

A. LaBar

The accused, appearing on his own behalf:

D. Wiwchar

Counsel appearing as Amicus Curiae:

T.M. Arbogast, K.C.

K.A. Kirkpatrick

Place and Date of Hearing:

Vancouver, B.C.

October 28, 2024

November 4 and 8, 2024

Place and Date of Judgment:

Vancouver, B.C.

November 27, 2024

- [1] These reasons for judgment were delivered as oral reasons. They have since been edited for distribution.

Introduction

- [2] This ruling addresses the Crown's application for summary dismissal of Mr. Wiwchar's abuse of process allegation outlined in Notice of Application 215 ("NOA 215") filed by his former counsel on June 7, 2024. Mr. Wiwchar's substantive application is grounded in his theory that the police services involved in this investigation unlawfully reviewed surveillance footage of him obtained from his attendances at the Edgewater Casino in Vancouver, B.C., on March 25, 26, May 22, and June 8, 2012. Surveillance security cameras at the casino were zoomed in on Mr. Wiwchar when he was logging in to his encrypted BlackBerry devices.
- [3] The applicant contends members of the Vancouver Police Department ("VPD") obtained the password to his BlackBerry device by slowing the zoomed video and repeatedly watching his fingers as he entered the password. Mr. Wiwchar contends that this is how the police obtained the password to his devices and that they unlawfully reviewed his BlackBerrys following his arrest in Toronto, Ontario, on June 21, 2012. Mr. Wiwchar further contends that the police then concocted a cover story to obscure the fact that they already had his passwords and had access to his devices.
- [4] The cover story as alleged by Mr. Wiwchar is what the Crown argues is the true state of affairs: prior to June 2014, the Toronto Police Service ("TPS") and the RCMP had no way to access Mr. Wiwchar's encrypted BlackBerry devices.

- [5] In response to NOA 215, the Crown argues Mr. Wiwchar's allegations of abuse are unfounded. Moreover, the Crown contends that there is nothing in the way of a "showing of evidence" which, if assumed true, could substantiate Mr. Wiwchar's theory that the police engaged in a coverup.
- [6] On this preliminary application, relying on the framework established in *R. v. Haevischer*, 2023 SCC 11 ("Haevischer"), the Crown seeks summary dismissal of Mr. Wiwchar's abuse of process application in respect of video surveillance footage taken in the Edgewater Casino in Vancouver, B.C. in May and June 2012 ("NOA 215").
- [7] In *Haevischer*, the Supreme Court of Canada remitted Mr. Haevischer's stay of proceedings application (which alleged abuse of process) back to the trial court for a hearing on the merits of the application. Justice Martin, writing for a unanimous court, explained that an application in a criminal trial should only be summarily dismissed if it is "manifestly frivolous".
- [8] In NOA 215, and in his October 18, 2024, argument, Mr. Wiwchar relies on both the trial fairness and residual categories of abuse of process as set out by the Supreme Court in *R. v. Babos*, 2014 SCC 16.

Background facts

- [9] Mr. Wiwchar faces two charges on Indictment 27393: one count of first-degree murder and one count of conspiracy to commit murder. In respect of the charge of first-degree murder, the allegation is that Mr. Wiwchar shot and killed Sandip Duhre in a restaurant inside the Wall Centre Hotel in Vancouver, B.C. The shooting occurred on the evening of January 17, 2012.
- [10] The alleged shooter of Mr. Duhre could not be identified by his facial or physical features. The movements of the shooter were caught on various surveillance cameras within and around the Wall Centre Hotel, but identification of the shooter from the images is unlikely.
- [11] The Crown's case against Mr. Wiwchar is circumstantial.
- [12] In that vein, a significant portion of the Crown's case against Mr. Wiwchar lies in the text messages extracted from a number of cellphones seized in the course of the investigation. Mr. Wiwchar was originally tried with two co-accused, Larry Amero and Rabi Alkhalil. Midway through the joint jury trial, Madam Justice Maissonville severed Mr. Wiwchar from the trial after he dismissed his counsel. Severance was effected on March 7, 2022.
- [13] The trial of Amero and Alkhalil continued before the jury. Midway through the Crown's closing address, Alkhalil escaped from the correctional centre where he was detained. The trial continued. Mr. Amero was convicted by the jury, as was Mr. Alkhalil, albeit in absentia.

- [14] Following Mr. Duhre's murder, Mr. Wiwchar became a suspect in the investigation when members of the VPD became aware that Mr. Wiwchar was associated with a grey Mazda MPV that matched the vehicle that drove the shooter to the scene of the murder. Once Mr. Wiwchar became a suspect in Mr. Duhre's death, he was placed under continuous surveillance by members of the VPD Strike Force Unit surveillance team.
- [15] The Crown in its reply to NOA 215 has fairly summarized the factual circumstances surrounding the investigation of Mr. Wiwchar as it pertains to observations of him in the Edgewater Casino in the spring of 2012, Mr. Wiwchar's arrest in Toronto, Ontario, on June 21, 2012, the devices seized from Mr. Wiwchar's custody when he was arrested, and the process employed to try and gain access to Mr. Wiwchar's devices:
6. On March 25, 2012, the surveillance team followed Mr. Wiwchar into the Edgewater Casino located at 750 Pacific Boulevard in Vancouver (the "Casino"). Members attended the CCTV video monitoring room to continue their surveillance. The area was used by Casino staff to monitor activities on the Casino floor, using a number of CCTV video cameras placed throughout the premises, some of which had zoom-in capabilities.
 7. One of the surveillance team members, Cst. Berceanu, was in the CCTV video monitoring room directing Casino staff to focus the cameras on Mr. Wiwchar. From the late evening hours of March 25, 2012 until the early morning hours of the following day, Mr. Wiwchar was observed gambling and standing in the Casino. On two occasions the CCTV video cameras zoomed in on him while he was using a BlackBerry and sending text messages. The police did not have a judicial authorization to read the messages displayed on Mr. Wiwchar's BlackBerry on this date.
 8. On March 27, 2012, Detective Dungey of the VPD attended at the Casino and requested the CCTV video footage from the two prior days, depicting Mr. Wiwchar inside the Casino.
 9. On March 28, 2012, Detective Dungey returned to the Casino and recovered a hard drive with the requested CCTV video footage from March 25 and 26, 2012. He reviewed the CCTV video footage and observed Mr. Wiwchar sending and receiving text messages. Detective Dungey noted that when Mr. Wiwchar received a message on his BlackBerry, a message appeared which read, "Decoding PGP Message". Likewise, when Mr. Wiwchar typed out his message a message appeared which read "Encoding" in a banner across the top of the screen and a second message below that read "PGP Universal Default". There is no evidence Detective Dungey observed Mr. Wiwchar's password to unlock his BlackBerry, nor is there evidence that such an observation was made by any other member who also reviewed the Casino CCTV video footage.
 10. On March 29, 2012, the police obtained a production order for the March 25 and 26, 2012 Casino CCTV video footage. They also obtained a general warrant to allow them to use the CCTV video cameras at the Casino to covertly read the messages being sent and received by Mr. Wiwchar in the future.

11. On June 1, 2012, the police obtained a second general warrant which mirrored the first. The two general warrants were used to obtain CCTV video footage of Mr. Wiwchar at the Casino on May 22 and June 8, 2012.
12. In total, the police obtained video footage of Mr. Wiwchar at the Casino in respect of four days (three visits), those being March 25-26, May 22, and June 8, 2012.
13. On June 21, 2012, Mr. Wiwchar was arrested by members of the Toronto Police Service (TPS) for the murder of John Raposo while he was in passenger in a taxi in downtown Toronto. Mr. Raposo had been shot and killed three days earlier while dining on a patio of a café on College Street.
14. Incidental to Mr. Wiwchar's arrest, the police seized four electronic devices: three BlackBerrys and one Nokia cellphone. One of the BlackBerrys, later determined to be a BlackBerry Bold 9900, was recovered from the backseat of the taxi; the remaining two BlackBerrys, later determined to be BlackBerry Bold 9360s, were recovered from a bag in the trunk of the taxi.
15. A warrant was obtained on June 27, 2012 to search the four electronic devices.
16. The Nokia cell phone was found to contain no data. The three BlackBerrys were all password protected and required the assistance of the RCMP Technical Analysis team (TAT) in Ottawa for technical support.
17. The BlackBerry Bold 9900 was sent to TAT in Ottawa where a chip-off extraction of the device's internal memory chip was performed on August 20, 2012. However, the analysis of the device was not completed because the device had been "wiped" (i.e., the user-created data on the device had been completely erased).
18. With respect to the two BlackBerry Bold 9360s found in the bag in the trunk of the taxi, the police did not have the technological solution to gain access to them in June 2012.
19. It was not until two years later, in June 2014, that the RCMP Technical Crime Unit (TCU) invited the TPS to resubmit those particular devices as they believed they had developed a technological solution to the encryption barriers.
20. On July 18, 2014, a second warrant was obtained to search the BlackBerry Bold 9360s. The devices were then sent to TAT in Ottawa for analysis.
21. On December 18, 2014, C/M Kim Warren, a forensic hardware engineer at TAT, was able to obtain a partial read for password hash extraction with respect to both devices using a new in-circuit technique (considered to be a sensitive protected police technique). Under C/M Warren's supervision, C/M Anthony Fuentes had disassembled the two devices, removed the radio frequency shield, and wired them up to the in-circuit extraction equipment. The devices were processed, and a partial read of the device's memory for password hash and PGP certificate were obtained. The devices were then reassembled and repackaged.

22. The next day, acting Operation NCO at TAT, S/Sgt. Nicolas Bernier used what C/M Warren had obtained through the in-circuit extraction process, to extract the actual passwords hashes for the BlackBerry Bold 9360s content protection and "Key Store" application (the steps he took to uncover the passwords are discussed in more detail below).
23. On January 6, 2015, C/M Sean Emack, a technical forensic analyst at TAT, completed triage of the BlackBerry Bold 9360s and data extraction using the passwords obtained by S/Sgt Bernier.
24. The devices were then returned to TPS to complete the process of manual extraction (screenshots) since the file system for these devices did not support alternative means of analysis including the application of the RDX forensic tool. During this process, the police learned that both devices had PGP email accounts, the details of which are as follows:
 - TAT# T2012-129-002 / TPS# N954543 - a white BlackBerry Curve 9360, with PGP email account, WrathOfTitans@platinumsecure.tv
 - TAT# T2012-129-003 / TPS# N954545 - a black BlackBerry Curve 9360, with PGP email account, ManVFood@platinumsecure.tv
25. The WrathOfTitans PGP email account contained highly incriminating evidence relevant to the Raposo murder, the Duhre murder and the Dhak murder conspiracy. The ManVFood PGP email account had additional messages relating to the Dhak murder conspiracy.
- ...
40. As stated previously, it was S/Sgt Bernier who, through the use of in-circuit extraction methods performed by C/M Warren, was able to extract the password hashes to unlock the BlackBerry Bold 9360s (content protection) as well as the Key Store (PGP encryption). S/Sgt Bernier testified in the previous trial, post-Wiwchar severance, about matters related to PGP encryption, but was never asked about this particular issue. However, he did provide a will say statement dated June 10, 2016, outlining the steps he took.
41. In that will say statement, he declared:

This statement made by me accurately sets out the evidence which I would be prepared, if necessary, to give in court as a witness. The statement is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have willfully stated in it anything which I know to be false or do not believe to be true.

He then stated:

On December 18th, 2012 the two BlackBerry devices were processed by TIS TAT laboratory civilian member Kimberly Warren using an in-circuit technique. The in-circuit technique is a sensitive protected police technique developed by TIS TAT

WILL SAY

On December 19th, 2014 as part of the in-circuit technique process and as my role as the acting operations non-commissioned officer (Ops NCO):

- I extracted the required password hashes for both devices from the partial data read of each device's memory.
- I noted that both devices had identical password hashes for both the device password and the Keystore application password.
- I resolved the password hashes to their plaintext equivalent of "seawater".
- I did not take possession of the BlackBerry devices at any point during my involvement.
- I assigned civilian member Sean Emack with completing the remaining triage and return of both BlackBerry devices.

He concluded the will say by signing and dating it.

42. In a Task Action Report (TAR) dated March 11, 2019, Det. Hans Dykman, at the request of the defence, made further inquiries as to how S/Sgt. Bernier obtained the passwords for Wiwchar's devices, and the process/software used. He advised that on March 8, 2019, he received a response from NCO Cpl. Jean-Sebastien Fortier, in charge of the TAT (S/Sgt Bernier was no longer employed with TAT by that time), which stated in part:

When performing digital forensic analysis of BlackBerry devices, the Technical Analysis Team (TAT) employs different technique workflows. In this case, the technique workflow involves the use of electronic lab equipment to obtain electrical access to the memory chip in order to extract the unencrypted data that represents the hash values of the device's access passwords. Since the user data on the device is encrypted and cannot be decrypted outside of the device, this workflow does not extract all of the data from the device. Only a sufficient amount of data is extracted that can be used to identify the hash values (or "hashes") that represent:

- (a) the password required to unlock the BlackBerry device and permit the device to display decrypted content (that is, content that is encrypted using "Content Protection"), and;
- (b) the password required to decrypt portions of the PGP key contained in the BlackBerry device.

The advantage of this workflow is that it does not require the removal of the chip from the device and leaves the device in a functional state. Once the data that can identify the hash values is extracted from the memory chip, efforts are performed to determine the passwords noted above in "a)" and "b)" (*see note below). After these passwords are determined, they are used by a TAT analyst (in an area that is isolated from electromagnetic radiation) to enter the passwords into the powered device when prompted on-screen, so that the device contents and PGP email messages (if present) can be perused on the device, and photographed as necessary. This process of interacting with the device by the TAT analyst is performed to ensure that everything has been

accounted for, such that a TAT Crime analyst in a Tech Crime Unit will be able to perform a manual analysis of the active data present in the BlackBerry device.

*Note: The details regarding the equipment, tools, and techniques employed to determine password is considered to be privileged by the RCMP.

43. Of note, there is no evidence that S/Sgt Bernier spoke to any VPD officer in order to obtain the password.
- [16] As S/Sgt. Bernier explained in his evidence on the voir dire for NOA 198 (the expert evidence voir dire) TAT only accepted devices that referring police agencies could not access due to the encryption features and the lack of access to the password for the device. If the referring force had a way to access the device, for example, the passwords, TAT would not accept the device for analysis.
- [17] In the case of Mr. Wiwchar's two devices, WrathOfTitans and ManVFood, S/Sgt. Bernier was clear in his evidence, he obtained the passwords for the devices through the in-circuit extraction method, where enough memory was extracted to obtain the hash values or scrambled strings for passwords. The passwords were then resolved through an open-source program known as OCL Hashcat used to crack the passwords by descrambling the string of code. Staff Sergeant Bernier was able to use this software and extract the passcodes for each device. The passcodes for the devices and their Keystore access passcodes were the same: "seawater". Staff Sergeant Bernier did not speak to any of the investigators assigned to the case prior to resolving the passwords for the devices. In other words, nobody from VPD or TPS told him what the passwords were, for good reason: nobody knew them until S/Sgt. unscrambled them on December 19, 2014.
- [18] It is important to understand that NOA 215 is not Mr. Wiwchar's first challenge to the circumstances surrounding the surveillance videotapes from the Edgewater Casino. It is, however, the first time in the 12-year history of this case that he has alleged that the police had his BlackBerry passwords since the inception of the investigation.
- [19] When he was arrested in Toronto on June 21, 2012, Mr. Wiwchar was charged with a number of firearms offences in Vancouver, B.C. A co-accused, Philip Ley, was added to the indictment. Mr. Wiwchar and Mr. Ley were tried in this Court by Justice Bowden. On this summary dismissal motion, the Crown argued the following with respect to these prior proceedings in its reply submissions to Mr. Wiwchar's NOA 215:
45. Mr. Wiwchar challenged the admissibility of the text messages which were observed by the police on March 25 and 26, 2012, prior to obtaining judicial authorization. He did not challenge any of the other evidence contained on the hours of Casino CCTV video footage. Nor did he challenge any of the evidence obtained on May 22 and June 6, 2012 pursuant to the two general warrants previously mentioned.

In a ruling indexed as R. v. Ley, 2014 BCSC 2108, Bowden J. held that Mr. Wiwchar had a reasonable expectation of privacy in his text messages, and that the seizure without prior judicial authorization constituted a breach of his s. 8 Charter rights. He also excised the text messages from the subsequent ITOs.

46. Bowden J. also held that Mr. Wiwchar did not have a reasonable expectation of privacy in the balance of the observations the police made with the use of the Casino CCTV video footage:
25. I will first consider whether the applicant had a reasonable expectation of privacy in the casino.
26. The police frequently use surveillance techniques, including cameras with a zoom function, to follow and photograph suspects. An example is found in R. v. Bryntwrick, 2002 CanLII 10941 (Ontario Superior Court), where the police surreptitiously videoed an accused walking from the front door of his residence to the garage. The court held that did not infringe his s. 8 rights.
27. The case before me is different. I do not consider that the applicant had an expectation of privacy in the casino with regard to his personal appearance including such things as his visage, his posture, his gait and the clothing that he wore. Nor did he have an expectation of privacy in relation to his actions while participating in a game.
- [20] There was no suggestion in the trial before Justice Bowden that the VPD investigators had watched the casino surveillance videos and ascertained the passwords for Mr. Wiwchar's devices through repeatedly watching the videos of Mr. Wiwchar punching in his passwords while using the devices.
- [21] Following the firearms trial concluding before Justice Bowden, Mr. Wiwchar then stood trial in Toronto, along with Mr. Alkhalil, Nick Nero, and Martino Caputo. The four men were jointly charged with the first-degree murder of John Raposo. Following a jury trial, the four were convicted of first-degree murder on May 11, 2017, and sentenced to life imprisonment on June 27, 2017.
- [22] During the course of the Raposo murder trial, Mr. Wiwchar did not challenge the lawfulness of the forensic examination of the two BlackBerry Bold 9360 devices associated to him. No argument was advanced to support the theory that the police obtained the passwords for those devices through watching the casino surveillance tapes. The admissibility of the PGP messages found on the devices was not challenged. Indeed, Mr. Wiwchar, through counsel, made extensive admissions in the Raposo trial covering these areas.
- [23] After the proceedings in Toronto in respect of the Raposo murder concluded, Mr. Wiwchar was transferred back to B.C. to deal with the charges on this indictment before Justice Maisonville. As noted earlier, Mr. Wiwchar was jointly charged with Alkhalil and Amero.

- [24] Before Justice Maisonville, the Crown accepted Justice Bowden's rulings from the firearms trial. The Crown conceded a s. 8 Charter breach for the seizure of the March 25 and 26, 2012, text messages. The Crown further conceded that reference to these text messages should be excised from the ITOs. Finally, the Crown advised it would not be relying upon the text messages as observed on the casino's CCTV video footage for any purpose at the trial before Maisonville J. They maintain that position on the proceedings now before the Court.
- [25] Before Mr. Wiwchar was severed from the trial with Maisonville J., he challenged the admissibility of all the casino CCTV video capturing his movements on the property, irrespective of whether it captured him sending or receiving text messages. He argued he had a reasonable expectation of privacy in his image and that the police breached his s. 8 Charter privacy rights by using and reviewing the CCTV video from March 25 and 26, 2012, without prior judicial authorization.
- [26] The Crown responded to the application by relying upon the principles in *R. v. Vukelich* (1996), 108 C.C.C. (3d) 193. The Crown argued that Mr. Wiwchar had no reasonable expectation of privacy with respect to the CCTV video images captured of him at the casino. Moreover, the Crown argued this issue was previously decided by Justice Bowden in the firearms trial. In short, there was no merit in proceeding with a voir dire as the application had no prospect of success.
- [27] In a ruling indexed at *R. v. Alkhalil*, 2019 BCSC 1958 ("Alkhalil 1958") Justice Maisonville ruled in favour of the Crown and summarily dismissed Mr. Wiwchar's s. 8 Charter application. She found at paras. 38-51 of that ruling that Mr. Wiwchar had no personal, territorial, or informational privacy interests engaged by the impugned CCTV video footage and referred to a number of authorities in support of her ruling.
- [28] In the course of the hearing of this current application, at Mr. Wiwchar's request, extracts of the CCTV footage from the Edgewater Casino were marked as exhibits and were played for the Court. Mr. Wiwchar implored the Court to watch these videos again, in particular Video Q in Exhibit 11 and Video O in Exhibit Number 3. Mr. Wiwchar also contends that the Sequence 1 and Sequence 2 videos in Exhibit 3 establish, by being labelled "Sequence", that the VPD used the two video extracts to obtain his passwords for his BlackBerry devices.
- [29] Since the argument in Court, I have watched Video Q, Video O, Sequence 1, and Sequence 2 a number of times. I am satisfied that Sequence 1 and Sequence 2 are simply clips or extracts copied from Video O. The nomenclature of "Sequence" ties back to Exhibit 2 on this application, which is the relevant extracts from Detective Constable ("DC") Lisa Wu's ITO in support of an application, P3/2012, for an authorization to intercept communications as outlined at para. 390 of the ITO.

- [30] Paragraphs 388 and 389 of the ITO are also in Exhibit 2. It is clear from paras. 388-390 of the ITO that Det. Dungey of the VPD watched the CCTV footage from the Edgewater Casino and was able to observe aspects of the text messages being typed or received by Mr. Wiwchar. However, there is absolutely no evidence that any police officer in this investigation was actually able to see Mr. Wiwchar entering his password into his devices when sending or receiving encrypted messages.
- [31] Having reviewed the video extracts a number of times, I find that it is impossible to determine what the password is that Mr. Wiwchar enters when prompted to enter his Keystore access passcode.
- [32] I will address each video in turn.

Video O

- [33] This video starts at 23:59:23 hours on March 25, 2012, and ends at 01:04:59 hours on March 26, 2012, and is 117,930 frames in length. While the screen of the device is visible and the messages being typed at various points are more or less decipherable, whenever the Keystore access prompt is displayed on the device's screen and Mr. Wiwchar enters his password, it is impossible to discern what password he is entering for two reasons: (1) the text being inputted to the device in the access code only shows as asterisks; and (2) it is not possible to discern which keys on the BlackBerry device Mr. Wiwchar is pressing because his fingers obscure the keys on the device's keyboard.

Sequence 1 Video

- [34] This video appears to be a slightly clearer version of the footage in Video O. It is, however, the same video. The message being typed by Mr. Wiwchar is the "I zapped" message outlined in para. 388(b)(3) of DC Wu's ITO. Even with the seemingly clearer view of the screen, it is impossible to decipher the passcode that Mr. Wiwchar enters into his BlackBerry when prompted for the Keystore access passcode for the reasons outlined at para. 33 of these reasons.

Sequence Video 2

- [35] Like the Sequence 1 video, the Sequence 2 video is clearer than the overall Video O. It opens with Mr. Wiwchar reviewing the "I zapped" message, then inputting his Keystore access passcode, and then typing the, "Dude, I've been asking for a cop car" message outlined at para. 388(b)(5) of DC Wu's ITO. Again, when the Keystore access prompt appears on the device's screen, it is impossible to determine what password Mr. Wiwchar is inputting for the reasons previously outlined.

Video Q in Exhibit 11

- [36] This CCTV video is also from March 26, 2012, at the Edgewater Casino. It starts at 02:04:57 hours and ends at 03:04:59 hours. At approximately 02:43:05 hours or at the 38 minute and 10 second mark, Mr. Wiwchar can be seen using his BlackBerry and seemingly inputting a passcode. Again, it is impossible to discern what the passcode is as his fingers obscure the keys he is pressing on the device's keyboard and the figures on the screen of the device are too blurred to make out anything. And, at 02:46:44 hours or 41 minutes and 57 seconds into the hour-long video, Mr. Wiwchar can again be seen to be manipulating his BlackBerry device, entering some sort of password in response to what looks to be the Keystore access screen prompt. Again, however, nothing is discernible in the way of a password, because the screen is too blurred and Mr. Wiwchar's fingers obscure the keyboard of the device.
- [37] From having carefully reviewed these videos a number of times, I have no hesitation in finding that the VPD investigators could not and did not obtain Mr. Wiwchar's password to his BlackBerry by watching the CCTV videos from the Edgewater Casino.

Governing legal framework

- [38] In *Haevischer*, the Supreme Court of Canada determined that the threshold test for the summary dismissal of applications made in the criminal law context is whether the underlying application is manifestly frivolous. Justice Martin outlined the two core values relevant to a summary dismissal application: trial efficiency and trial fairness. In terms of efficiency, the main concern is the avoidance of disproportionate or undue delay: *Haevischer* at para. 51.
- [39] Trial fairness, a constitutional imperative, arises because summary dismissal runs counter to the notion that parties should have the opportunity to present their cases and to have the evidence, claims, and allegations adjudicated on their merits. Thus, trial fairness requires a low threshold for holding a *voir dire*: *Haevischer* at paras. 55-59.
- [40] In *Haevischer*, at paras. 68-69, Martin J. described the meaning of both "manifestly" and "frivolous". Importantly, the frivolous nature of the application must be obvious on the face of the record, otherwise the application should be heard.
- [41] In *Haevischer*, the court provided guidance on how to apply the manifestly frivolous threshold. This can be summarized in the following manner (all references to *Haevischer*):
- 1) The judge must assume the facts alleged by the applicant to be true and must take the applicant's argument at their highest. However, the applicant's underlying application should explain its full factual foundation and point towards anticipated evidence that could establish their alleged facts. Where the applicant cannot point towards any anticipated evidence that could establish a necessary fact, the judge can reject the factual allegation as manifestly frivolous: para. 83.

- 2) The judge ought to accept the inferences suggested by the applicant unless there is no reasoning path toward the inference: para. 83
 - 3) Determine if there is a fundamental flaw in the application's legal pathway such that the remedy is unattainable. For instance, the application may have put forward a legal argument that has already been rejected. Applications that "depend on legal propositions that are clearly at odds with settled and unchallenged law are manifestly frivolous": para. 85.
 - 4) Determine if the application creates a situation where the remedy sought could never issue on the facts of the particular application: para. 86.
 - 5) Determine if there are key portions or factual allegations missing from the application. Fundamental flaws must be manifest; i.e., apparent on the face of the record. If not, the underlying application must be allowed to proceed: paras. 87-88.
 - 6) The power to summarily dismiss is an ongoing power: para. 89.
 - 7) The burden is on the party seeking summary dismissal to establish that the application is manifestly frivolous: paras. 90-92.
 - 8) The party filing the underlying application must ensure it complies with the court's rules, practices, directives, and procedures: para. 94.
- [42] On this last point, in this province, CPD-3 is the practice direction that guides complex criminal cases, and para. 46 of CPD-3 provides:
46. At least 14 days before the application screening conference, the parties are to deliver to the other party and the Court written notice of each voir dire or pre-trial application they wish the Court to hear in the case. The written notice is to set out in detail
 - (a) the relief sought
 - (b) the basis in law on which it is sought
 - (c) the facts on which the applicant relies
 - (d) an overview of the evidence proposed to be adduced in support of the application, including the form of the evidence (for example, viva voce evidence, affidavits, agreed statements of fact, statements of counsel), and
 - (e) the time estimate for the voir dire or pre-trial application, and an explanation for the basis of the estimate (by reference to, for example, the direct examination and the cross-examination of each witness, submissions, etc.).
- [43] Paragraph 46(c) and (d) require that the applicant provide a detailed written notice of "the facts on which the applicant relies" and "an overview of the evidence proposed to be adduced in support of the application".

- [44] Justice Martin was also clear in *Haevischer* at paras. 93-98 that applications for summary dismissal of matters said to be manifestly frivolous are to be conducted on a minimal record and be of a summary nature, because extensive evidence often demands the type of time, effort, and delay that works to defeat the very purpose of the motion.
- [45] In other words, courts should not turn *Haevischer* motions into evidentiary hearings that involve examining and cross-examining witnesses. How a summary dismissal motion is conducted lies within the hearing judge's case management powers. As Justice Martin noted:
- [98] While counsel's statements will often be sufficient, sometimes more might be required. I leave it to the discretion of the judge deciding the summary dismissal motion to determine whether something more is required and, if so, what that something more should be. Deciding how the summary dismissal motion proceeds is within the judge's case management powers. However, the judge should bear in mind that the more material filed, the greater the risk of delay, the greater the risk that the summary dismissal hearing devolves into a scrum over the merits of the underlying application and the greater the risk that the judge inadvertently decides the merits of the application itself (*Gill* (BCSC), at para. 24).

Analysis

- [46] I begin by noting that the only sort of evidence Mr. Wiwchar has pointed to is the video footage from the Edgewater Casino. He contends it is obvious that the police obtained the password for his devices by slowing down the videos, repeatedly watching him enter his Keystore access passcode, and subsequently figuring out the password from the action of his fingers manipulating the device as he entered his passcode. The evidentiary basis for Mr. Wiwchar's underlying application is decidedly devoid of any sort of detail. Taken at its highest, Mr. Wiwchar's argument rests in his belief that the police are lying about how they accessed his BlackBerry devices. He argues that cross-examination of certain police officers, including DC Brown of the TPS, will assist in establishing his contention.
- [47] I note that there are troubling improprieties that have arisen within the investigations: the loss of two exhibits from the VPD exhibit locker (cellular devices known as 19LW and 58LW seized from Mr. Amero in Mr. Alkhalil's Montreal apartment) and their replacement with two imposter phones. However, Mr. Wiwchar's theory goes beyond this: he now believes that the VPD somehow obtained the passwords for his BlackBerry devices at the outset of this investigation, from March through May 2012, and accessed his devices shortly after his arrest in June 2012. He contends they committed this act two and a half years earlier than S/ Sgt. Bernier extracted the passcodes from them in his digital forensic analysis conducted in December 2014. He relies upon the videos that I have reviewed and summarized in the factual component of this ruling to support his contention that this is how the investigation obtained his passwords.

- [48] Respectfully, the evidence supporting Mr. Wiwchar's theory is decidedly to the contrary. The following facts must be remembered:
- 1) The Edgewater Casino CCTV videos on this application were seized by the VPD investigators in March 2012.
 - 2) Mr. Wiwchar's BlackBerry devices were seized incident to his arrest by the TPS on June 21, 2012, nearly three months after the CCTV surveillance video from the casino.
 - 3) There is no evidence that supports the theory that the VPD officers reviewed the Edgewater Casino videos to obtain the passwords from Mr. Wiwchar's devices. There is nothing in the ITO to support this. There are no officers' notes to support this. There are no task action reports. There is no evidence that the VPD obtained the password through watching the videos of Mr. Wiwchar at the Edgewater Casino. Indeed, having reviewed the videos in question, it is impossible to discern what password Mr. Wiwchar inputs into the devices as his fingers obscure the keys on the device's keyboard and the Keystore access prompt screen only shows asterisks when Mr. Wiwchar enters his password.
 - 4) There is no evidence that the VPD forwarded any password to the TPS between June 2012 and mid-2014 when Mr. Wiwchar's devices were resubmitted to the RCMP TAT unit to decrypt.
 - 5) There is no evidence to support the proposition that the TPS gained access to Mr. Wiwchar's devices and unlocked them with a recovered password prior to receiving the password that was extracted and recovered by S/Sgt. Bernier on December 19, 2014.
 - 6) Even if it was possible to discern what the Keystore access passcodes were for Mr. Wiwchar's devices from the videos of March 25 and 26, 2012, something I specifically rejected as impossible, there is no evidence to support the inference that the passcodes for the devices in March 2012 were the same in June 2012.
- [49] While the decision in *Haevischer* urges caution in resort to summary dismissal of applications, I am satisfied that Mr. Wiwchar's NOA 215 meets the *Haevischer* threshold of being manifestly frivolous.
- [50] While the Court is instructed to assume the facts alleged to be true and take the applicant's arguments at their highest, Mr. Wiwchar's underlying application is devoid of any factual foundation or any anticipated evidence that could establish the necessary facts. Rather, Mr. Wiwchar hopes that cross-examination of the officers might reveal something. I am of the opinion that this venture amounts to nothing more than a fishing expedition and I reject the purported factual allegations as manifestly frivolous.
- [51] The weight of the evidence before the Court on this application irrefutably establishes the exact opposite of Mr. Wiwchar's contention. The passwords to his devices were not obtained by watching the Edgewater Casino CCTV videos. To the contrary, they were obtained by S/Sgt. Bernier on December 19, 2014, through the process he described in his evidence.

- [52] In addition, given the evidentiary vacuum, that is the complete absence of evidence to support Mr. Wiwchar's allegation, there is no reasoning path toward the inferences he seeks. Indeed, there is not a scintilla of evidence adduced on this application that supports Mr. Wiwchar's contention that the investigators accessed his devices in 2012 at the time of his arrest. The evidence is completely to the contrary.
- [53] This court can make only one reasonable inference, which is based in fact and supported by the will-say statement of S/Sgt. Bernier and the related Task Action Report of Sgt. Dykman. Mr. Wiwchar's cellular devices were not accessible in 2012. Neither the VPD nor the TPS had the passwords for the devices and the RCMP did not have the technology to crack the passwords until 2014. Mr. Wiwchar's devices were not accessed until the RCMP TAT unit had the technology to do so and S/Sgt. Bernier applied it and extracted the passwords to Mr. Wiwchar's devices on December 19, 2014.
- [54] Insofar as NOA Number 232 is concerned, Mr. Wiwchar filed this application to cross-examine Det. St. Amant of the VPD and D/Sgt. Terry Browne of the TPS within the context of the Crown's Haevischer application on NOA Number 215. It appears to me that Mr. Wiwchar simply wanted to cross-examine the officers to purportedly establish some sort of factual basis for his allegations of police misconduct with respect to obtaining the password for his BlackBerry devices.
- [55] I have already established that this application is nothing more than a fishing expedition that is devoid of any basis in fact. The decision in Haevischer makes it clear that summary dismissal motions should be minimal and of a summary nature that do not devolve into a scrum over the merits of the underlying application: Haevischer at paras. 93-98 and 103-105.
- [56] Therefore, it is not necessary to hear from the two officers. Mr. Wiwchar cannot point to any evidence that they might provide that would advance his underlying application and so, in the exercise of my case management powers, I decline to permit cross-examination on this Haevischer motion. NOA 232 is dismissed.
- [57] Mr. Wiwchar's allegations of police misconduct relating to this application are completely unsubstantiated. His request for a voir dire in order to call witnesses is nothing more than a fishing expedition. Accordingly, the Crown's Haevischer application to have NOA 215 summarily dismissed is granted. Mr. Wiwchar has not provided any factual foundation to support his allegations and has failed to point to any anticipated evidence that could establish such a foundation. I have no hesitation in concluding that NOA 215 is manifestly frivolous.

Post-script

- [58] Following the conclusion of the hearing of the Crown's motion for summary dismissal motion of NOA 215, indeed after I had finished writing this ruling but before delivering it, Mr. LaBar for the Crown advised the Court on November 26, 2024, that Justice Maissonville had issued a Vukelich ruling on a similar application by Mr. Wiwchar prior to him being

severed from the indictment. Mr. LaBar advised the Court of this ruling during the course of his submissions addressing a facet of NOA 214, Mr. Wiwchar's application for a stay of proceedings based on an alleged breach of his s. 11(b) Charter right to a trial within a reasonable time.

- [59] I was unaware that a similar application had been summarily dismissed by Justice Maisonville. In *R. v. Alkhalil*, 2021 BCSC 37 ("Alkhalil 37"), Justice Maisonville summarily dismissed Mr. Wiwchar's NOA 71, wherein the defence challenged the manner of the search of Mr. Wiwchar's devices by alleging a s. 8 Charter breach. The defence sought the exclusion of the evidence obtained from the BlackBerry devices seized from him incidental to his arrest.
- [60] I note that this challenge related to different days of CCTV video from the Edgewater Casino, and one VPD officer's attempt to see if he could discern the password being entered into the device as shown in the June 8, 2012, video, that observation bore no fruit. The VPD and the TPS were not able to get into Mr. Wiwchar's BlackBerry devices prior to S/Sgt. Bernier's examination of them at TAT and extraction of the password hashes on December 19, 2014.
- [61] In *Alkhalil 37*, Justice Maisonville set out Mr. Wiwchar's position at paras. 16, 17, 22, and 23:
- [16] The applicant seeks an evidentiary hearing to establish that the manner in which his devices were searched was not reasonable and, therefore, contrary to s. 8 of the Charter. There are two components to his allegation:
- a) The use of video footage from the Edgewater Casino to attempt to obtain the password to his devices, and subsequent attempts by the TPS to access his devices in January 2013; and
 - b) The use of the Edgewater Casino video footage by the RCMP to decrypt his password in December 2014.
- [17] The factual basis the applicant puts forth for these allegations is as follows:
- a) On multiple occasions, the VPD made unlawful observations of his text messages, including his password, by means of the security cameras at the Edgewater Casino;
 - b) The VPD provided the results of those observations to the TPS, who seized the applicant's devices incidental to his arrest for the Raposo murder; and
 - c) The TPS and RCMP technical examiners attempted to gain access to the applicant's devices using passwords they obtained from the Edgewater footage.
- ...
- [22] The applicant's challenge to the search of his BlackBerrys has two components:
- a) Use of Edgewater footage to try to obtain the password to his devices and subsequent attempts by the TPS to access the devices in January 2013; and

b) Use of Edgewater footage by the RCMP to decrypt his password in December 2014.

[23] As set out above, the applicant relies on the following factual basis for his challenge:

- a) On multiple occasions, the VPD made unlawful observations of his text messages, including his password, by means of the security cameras at the Edgewater Casino;
- b) The VPD provided the results of those observations to the TPS, who seized the applicant's devices incident to his arrest for the Raposo murder; and
- c) The TPS and RCMP technical examiners attempted to gain access to the applicant's devices using passwords they obtained from the Edgewater footage.

[62] Justice Maisonville noted that on the dates in question in the application before her - May 22 and June 8, 2012 - the observations by investigators with the VPD of the video footage were authorized by general warrants:

[26] Accordingly, the allegation that the VPD made unlawful observations of the applicant's text messages and password flies in the face of the available information, with the exception, of course, of the conduct that was the subject of Bowden J.'s ruling.

[63] Justice Maisonville rejected the defence contention that the TPS shared information obtained from the Edgewater Casino CCTV video footage with the RCMP analysts to gain access to Mr. Wiwchar's devices: Alkhalil 37 at para. 27. She also rejected the foundational premise of Mr. Wiwchar's application that the police used and shared unlawfully-obtained video footage from the Edgewater Casino to gain access to his devices: Alkhalil 37 at para. 28.

[64] Additionally, Justice Maisonville concluded that there was no reasonable basis to suggest that the Edgewater Casino footage was used by the RCMP to decrypt Mr. Wiwchar's password. Rather, the devices were decrypted by the RCMP TAT unit using its developed technology, and not any information purportedly gleaned from the video footage: Alkhalil 37 at para. 30.

[65] Justice Maisonville's findings and conclusions accord with my own assessment of NOA 215 and the absence of any foundation or plausible evidence to support Mr. Wiwchar's theory that the police gained access to his devices using his passwords that they had obtained through watching him enter it while at the Edgewater Casino. Accordingly, Justice Maisonville's ruling reinforces my own conclusion that there is no purpose in proceeding to hear NOA 215 and the Crown's Haevischer application is granted.

"Ker J."

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/24/24/2024BCSC2442.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/r-v-wiwchar-2024>

Prepared on 27 October 2026 · Esheria