SUPREME COURT OF YUKON

Citation: *R v Smeeton*, 2024 YKSC 19

Date: 20240411
S.C. No. 22-01519
Registry: Whitehorse

BETWEEN:

HIS MAJESTY THE KING

AND

KOLE SMEETON

Publication, broadcast or transmission of any information that could identify the complainant or a witness is prohibited pursuant to s. 486.4 of the *Criminal Code*.

Before Justice K. Wenckebach

Counsel for the Crown	Adrienne Switzer (by videoconference)
Counsel and Agent for the Defence	David C. Tarnow (by videoconference)

This decision was delivered in the form of Oral Reasons on April 11, 2024. The Reasons have since been edited for publication without changing the substance.

REASONS FOR DECISION

[1] WENCKEBACH J. (Oral): The accused, Kole Smeeton, is charged with possessing, accessing, and making child pornography.

[2] The RCMP began its investigation into Mr. Smeeton after it received information from the National Centre for Missing and Exploited Children ("NCMEC"). Dropbox, a file hosting service, had informed NCMEC that a person with the username "Kole Smeeton" had uploaded a video of apparent child pornography on its service. Dropbox also

provided the IP address that uploaded the file. NCMEC did a search that allowed it to find the approximate location and internet service provider for the IP address, which it also provided to the RCMP.

[3] Following up on this information, an RCMP officer, Cst. Clements, emailed an employee of Northwestel and asked whether he could confirm that Northwestel was in possession or control of the IP address on the date the child pornography was uploaded. The employee confirmed that Northwestel had details for the IP address. He also stated that the ISP number was active and that it was issued in the Whitehorse area.

[4] Based on that information, the RCMP officer applied for and received a production order for information, including the subscriber information, about the IP address.

[5] The RCMP then sought a warrant to search the home associated with the subscriber who was assigned the IP address. Cst. Clements, who swore the ITO, identified the subscriber who was assigned the IP address, as well as his residential address. The subscriber was not Mr. Smeeton, but the ITO stated that there was evidence Mr. Smeeton lived at the residence where the IP address was assigned. The ITO did not contain information about whether the Wi-Fi was password protected or whether others may have access to the internet at the home. A judge granted the warrant.

[6] The RCMP thus searched the home. During their search, the police seized several electronic devices. They then obtained a warrant to search the electronics. In the execution of that warrant, they uncovered alleged child pornography.

[7] Mr. Smeeton now brings an application alleging that his rights under s. 8 of the *Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982* (the "*Charter*") were violated, and that the production order and search warrants should be quashed.

[8] The remedy he seeks is that the evidence collected pursuant to the warrants be excluded or, alternatively, that there be a stay of proceedings.

[9] The issues Mr. Smeeton raises are:

1. Did the inquiry about whether Northwestel held the ISP number violate Mr. Smeeton's rights under s. 8 of the *Charter*?
2. Was there a sufficient basis to issue the warrant?
3. Should the search warrants be set aside on the basis that the issuing judges did not review the ITOs sufficiently?

[10] I now turn to my analysis of the issues.

[11] With regards to the first question, Mr. Smeeton submits that his rights under s. 8 were violated when Cst. Clements asked Northwestel if it held the ISP number.

[12] Mr. Smeeton argues that there were two pieces of information Northwestel gave to Cst. Clements to which privacy interests are attached, that is, the ISP number was active and that it was issued in the Whitehorse area. He submits that Northwestel should not have voluntarily provided the information to Cst. Clements.

[13] I will start by setting out the pertinent legal principles on searches. I will then address the argument.

[14] Section 8 applies where a person has a reasonable privacy interest in the object or subject matter of the state action and the information to which it gives access (*R v Marakah*, 2017 SCC 59 ("*Marakah*") at para. 10).

[15] The factors used to assess whether there is a reasonable expectation of privacy include:

- the subject matter of the alleged search;
- whether the claimant had a direct interest in the subject matter;
- whether the claimant had a subjective expectation of privacy in the subject matter; and
- whether the claimant's subject expectation of privacy was objectively reasonable (*Marakah* at para. 11).

[16] The Court, in coming to its conclusion, must consider the totality of the circumstances. I will now address each factor in turn.

[17] First is the subject matter of the alleged search.

[18] The Supreme Court of Canada has explained that to get to the heart of the subject matter of the search, the Court must ask what the police were really after in conducting the search (*R v Bykovets*, 2024 SCC 6 at para. 34).

[19] In the case at bar, even before answering this question, it is necessary to clarify what the police literally sought from Northwestel. This is because Mr. Smeeton's counsel submits that what is problematic was that Northwestel told the police that the ISP number was active and that it was issued in the Whitehorse area. However, Cst. Clements did not ask Northwestel if the ISP number was active or where it was issued. The Northwestel employee who answered Cst. Clements' question volunteered

that information on his own. What Cst. Clements asked was whether Northwestel held the ISP number.

[20] What I must assess is not the information Northwestel volunteered but what Cst. Clements asked for. Thus, here, the issue is what Cst. Clements was really after when she asked whether Northwestel held the ISP number.

[21] The Crown submits that, in making that inquiry, Cst. Clements was seeking the correct entity upon which to serve the production order. I agree. Cst. Clements' question was narrow and specifically directed at ownership of the ISP number. That information permitted Cst. Clements to serve the production order on Northwestel.

[22] The second factor is whether Mr. Smeeton had a direct interest in the subject matter.

[23] Mr. Smeeton's counsel concedes that Mr. Smeeton's interest in the subject matter was tangential, at best. I would go further: I conclude that Mr. Smeeton had no interest in the subject matter.

[24] Northwestel is the entity with a direct interest in the subject matter because it owned the ISP number. The subscriber to whom Northwestel assigned the ISP number may also have an interest in the subject matter. That need not be decided here, however, as the subscriber was Mr. Smeeton's landlord, not Mr. Smeeton himself.

[25] Mr. Smeeton's link to the ISP number is through his landlord. The landlord gave Mr. Smeeton access to his Wi-Fi, which in turn meant that Mr. Smeeton accessed the internet through the ISP number.

[26] I cannot see any interest that Mr. Smeeton has in who possessed the ISP number, especially given that the RCMP's reasons for asking about it was to serve a production order on the owner.

[27] The third factor is the subjective expectation of privacy.

[28] Mr. Smeeton provided no evidence that he had an expectation of privacy in who owned the ISP number. It is also not self-evident that a third party using the ISP number assigned to a subscriber would have a subjective expectation of privacy.

[29] I therefore conclude that Mr. Smeeton did not have a subjective expectation of privacy in the subject matter of the search.

[30] As Mr. Smeeton has not established a subjective expectation of privacy, I need not consider the final factor of objective reasonableness.

[31] I conclude that Mr. Smeeton did not have a reasonable expectation of privacy in the RCMP's question to Northwestel. Section 8 therefore does not apply in the case at bar.

[32] The second question to be resolved is whether there was a sufficient basis to issue the warrant.

[33] Mr. Smeeton argues that the warrant should not have been issued because the police did not conduct sufficient investigations to determine that it was Mr. Smeeton that accessed the alleged child pornography. He also submits that the information was too dated. The warrant, therefore, lacked sufficient grounds to justify a search. The warrant should be quashed.

[34] As I am reviewing the authorization, before addressing the arguments, it is useful to discuss the standard of review I must apply. This is not a re-hearing of the application

for the warrant, nor can I substitute my view about whether the warrant should have been granted for that of the authorizing judge. Rather, I can quash the warrant only if there was no basis upon which I am satisfied that the pre-conditions for granting the authorization existed (*R v Araujo*, 2000 SCC 65 at para. 51). Put in other words, I must determine if there was "at least some evidence that might reasonably be believed on the basis of which the authorization could have issued." (at para. 51)

[35] Turning now to the analysis of the issues, Mr. Smeeton submits that the police should not have sought a search warrant without further investigating who downloaded the impugned video. The police had information that the ISP number associated with the home in which Mr. Smeeton lived had been used to download pornography. They did not know and did not take investigative steps to determine whether Mr. Smeeton's landlord may have been the person who downloaded the file or whether it was someone else, such as a visitor or even a neighbour accessing the landlord's Wi-Fi without permission. Defence counsel submits that because the police did not take these steps, the ITO was insufficient and should not have been issued.

[36] I am not convinced by this argument. When seeking a search warrant for a place, the police are not obligated to show that they can tie the offence being investigated to a particular suspect. Rather, what the police must establish is reasonable and probable grounds to believe that evidence in relation to an indictable offence would be located in the place the police seek to search (*R v Cusick*, 2019 ONCA 524 at para. 111).

[37] In the case at bar, the police had evidence a video of apparent child pornography had been uploaded and were able to link it to a residence through the ISP number associated with a subscriber at the residence. They also had information that the folder

in which the video was saved had Mr. Smeeton's name on it. Further, there was evidence that Mr. Smeeton lived at the residence. This all provided reasonable and probable grounds that evidence of an indictable offence would be located at the place the police were seeking to search.

[38] Moreover, generally, the issuing justice and reviewing judge should not question what investigative steps the police could have or should have taken before seeking a search warrant. The police are to be judged on "what they did, not what they could have done" (*R v Le*, 2021 BCCA 52 at para. 47). There are some exceptions to this principle, but Mr. Smeeton did not argue that they applied here. Whether the police should have approached the landlord or further investigated who accessed the landlord's Wi-Fi is not for me to decide.

[39] The police had reasonable and probable grounds articulated in the ITO and the authorization is therefore valid on that ground.

[40] Mr. Smeeton's second argument is that the information was too dated to be relied upon. The tip was received approximately four months before the police applied for the search warrant. Because of the delay in seeking the search warrant, Mr. Smeeton submits, the police did not have reasonable and probable grounds that the evidence would be at the residence at the time the search was to be conducted.

[41] The Crown submits that the information was not too dated to be relied upon. She argues that the ITO Cst. Clements provided included information about the tendencies of child pornographers, including that they tend to keep large amounts of pornography or erase and then download the pornography again. This supports the conclusion that the video would still have been on the electronic device at the time of the search.

[42] I agree with the Crown that the information was not too dated. However, my reasoning is different than that of the Crown. I decline to rely on the information in the ITO that describes the tendencies of child pornographers. I recently issued a decision in another case, *R v S*, 2024 YKSC 17 ("*S*"), in which defence, like here, challenged a search warrant issued to search a residence for evidence of a child pornography offence. The ITO contained passages that were very similar, or the same, as the paragraphs in this ITO that describe the proclivities of child pornographers. In *S*, I ruled that the police should not have included those paragraphs. I based my analysis on the Supreme Court's decision in *R v Morelli*, 2010 SCC 8 ("*Morelli*").

[43] In *Morelli*, the Supreme Court considered an ITO that included information about the tendencies of child pornographers. The Court noted that people who commit child pornography offences are not all one "type" of person. It then stated:

> [78] … the "propensities" of one type [of person who commits child pornography offences] may well differ … from the "propensities" of others. There is no reason to believe, on the basis of the information in the ITO, that *all* child pornography offenders engage in hoarding, storing, sorting, and categorizing activity. And there is nothing in the ITO that indicates which specific subset of … offenders [do] generally engage in those [behaviours]. (emphasis in original)

[44] The Court went on to admonish that ITOs should not contain "broad generalizations about loosely defined classes of people" (at para. 79).

[45] Although the defence did not take the position in this application that the paragraphs describing the tendencies of child pornographers should have been excised, given *Morelli* and my previous decision, I conclude it would not be appropriate to use the information in this case.

[46] What I can rely on, however, is information in the ITO of how information about computers and how documents are saved and deleted on computers may still be found. Cst. Clements affirmed that computers automatically save information, such as chat logs and images, to various locations in a computer system; when a user deletes information, the information is not necessarily permanently removed; and that forensic analysis can extract information that the user does not know exists on it.

[47] I take from this that information that has been deleted from a computer is not necessarily erased and may still be recovered. Here, then, even if the video were deleted, there are grounds to conclude that it could be extracted from another location in the computer system.

[48] Defence counsel also referred to cases in which information about the location of stolen goods was considered stale-dated a month after it was received in support of his position. However, cases involving drugs or stolen goods are not the same as cases involving child pornography (*R v Treloar*, 2022 ONCJ 121 at paras. 42-43). The former involved goods that are meant to be sold or passed on. Child pornography found on electronic devices, however, can continue to exist even after having been sent to another device. It is meant to be viewed and may be re-accessed. Depending on the facts, courts have determined that a delay of months, and even over a year, does not render information about uploading child pornography stale.

[49] In this case, the ITO stated that the video had been uploaded to Dropbox. It also explains that Dropbox is a file hosting service offering cloud storage, file synchronization, personal cloud, and client software. It would have been better had the ITO further explained what occurs when a person uploads a video to Dropbox.

However, there is enough information in the ITO to conclude that, when uploading a video to Dropbox, the user does not intend to delete it. This supports the inference that there was a similar intention here and that the information could still be available.

[50] There was evidence in the ITO that the video may have been retained and that, even if deleted, it could be recovered. The passage of four months did not, therefore, make the information too dated to be relied upon.

[51] I therefore conclude that there was a credibly based probability that evidence of a child pornography offence would be found at the residence, even though the police did not identify who was likely to have uploaded the video and even though the warrant was issued four months after the video of apparent child pornography had been uploaded.

[52] The next question is whether the search warrants should be set aside on the basis that the issuing judges did not review the ITOs sufficiently.

[53] Mr. Smeeton submits that the issuing judges did not take sufficient time to review the ITOs. As I understand it, counsel argues that this error not only supports the other arguments for quashing the search warrant but is also a standalone ground for finding the search warrants are invalid. Mr. Smeeton relies on *R v Emery*, 2019 BCSC 1710 ("*Emery*") in support of his submission.

[54] This argument arises from time notations on the ITOs and on the authorizations. The issuing judge marks on the ITO the time they received the document and, on the warrant, the time at which the judge authorizes the warrant.

[55] Here, on the first warrant, the judge wrote he received the ITO at 9:00 a.m. and also that he authorized it at 9:00 a.m. In the second ITO, another judge wrote that he received the ITO at 3:50 p.m. and authorized it at 3:55 p.m.

[56] The Crown submits that the presumption of regularity applies. It is presumed that the judges, as they are working in a public capacity, properly discharged their official duties (*R v Kapoor*, [1989] OJ No 1887 at para. 70). A party seeking to displace the presumption must establish on the balance of probabilities that it should not apply. The notations of the time showing no review or a short review is not sufficient to displace the presumption.

[57] The Crown also argues that even if the presumption does not apply, Mr. Smeeton has the burden of proof. This also requires him to demonstrate, on a balance of probabilities, that the judges erred in their review of the ITOs. Again, the notation of time is not sufficient to establish an error.

[58] Moreover, even if it could be established that the judges did not take enough time to consider the ITOs, Crown submits this does not lead to a reviewable error. The issue I must decide is whether the ITO contains some evidence that might reasonably be believed on the basis of which the authorization could have issued. Whether the judges properly reviewed the ITOs does not affect this analysis.

[59] I largely agree with the Crown. The presumption of regularity applies. Mr. Smeeton argues that the presumption applies to minor problems, such as misprints and typographical errors. It seems to me, however, that the presumption also applies to the manner in which an official discharges their duties. This includes the attention they pay to their duties. I am supported in my analysis by other courts who have also determined that the presumption of regularity applies in cases analogous to this case (*R v Maric*, 2019 ONSC 4478 at paras. 85-86).

[60] I further conclude that *Emery* is distinguishable. In *Emery*, the Court found that several parts of the ITO were facially problematic. It then excised several portions of the ITO. Given the context, it seems to me that the judge was indicating that the JJP could have, and should have, noted the deficiencies in the ITO. They did not, however, because of the haste with which they reviewed the document. That is not the case here, as I have determined that the first ITO, and subsequently, also the second, were valid.

[61] I also find, contrary to Mr. Smeeton's argument, that *Emery* did not determine that an issuing judge's failure to properly review an ITO provides a standalone ground for quashing a search warrant. Such a finding would run counter to the judge's role in reviewing the issuance of a warrant. The sufficiency of an ITO is based on its content, not on the amount of time a judge took to review it before issuing the warrant. I would therefore expect the Court in *Emery* to have engaged with this issue and provided a far more thoughtful analysis if it intended that the judge's lack of attention could form the sole basis for quashing a warrant.

[62] In coming to this conclusion, I am not saying that it is unimportant whether the authorizing judge reads the ITO with due care. Searches of homes and electronic devices provide the police with entry into the most private corners of a person's life. Authorizing judges are the gatekeepers safeguarding that the police will do this only when permitted by law. Invalidating a warrant after the fact is a poor substitute for ensuring that a search warrant is valid when it is issued. However, on these facts, even if I were to find that the judges had not reviewed the ITOs as they should have, this would not justify invalidating the warrants.

[63] I therefore uphold the issuance of the production order and the two search warrants. I dismiss Mr. Smeeton's application.

_____
WENCKEBACH J.