COURT OF APPEAL FOR ONTARIO

CITATION: R. v. West, 2020 ONCA 473
DATE: 20200722
DOCKET: C65919

Watt, Tulloch and Trotter JJ.A.

BETWEEN

Her Majesty the Queen

Respondent

and

Steven West

Appellant

Janani Shanmuganathan, for the appellant

Bradley Reitz, for the respondent

Heard: January 21, 2020

On appeal from the convictions entered on June 26, 2018 and the sentence imposed on November 5, 2018, by Justice Bernd E. Zabel of the Ontario Court of Justice.

Tulloch J.A.:

I. OVERVIEW

[1] The appellant, Steven West, was convicted of accessing, possession of, and distribution of child pornography.

[2] He appeals his conviction on the basis that his rights under s. 8 of the *Charter* were infringed and the evidence against him should be excluded pursuant to s. 24(2) of the *Charter*.

[3] For the following reasons, I would allow the appeal.

II. FACTS AND PROCEDURAL HISTORY

[4] At some point between the dates of August 21, 2016 and September 19, 2016, an image of child pornography was uploaded as the profile picture for an account on Kik, an instant messaging application for mobile devices.

[5] The image was detected by Kik and reported to the National Child Exploitation Coordination Centre, which proceeded to notify the Hamilton Police Service. The report contained the following pertinent details: the image had been uploaded between August 21, 2016 and September 19, 2016; it had been uploaded to an account with the username “mikeandvikes”, which had been registered on August 14, 2016; the image had been uploaded by an Android device, a Samsung Model SM-T530NU; and the first and last Internet Protocol (“IP”) addresses to be associated with the use of the account were 24.141.35.79 (“79”), and 24.141.102.67 (“67”), respectively. The report also included disclaimers stating that the information it contained had not been verified by Kik.

[6] From the report, the police were able to determine that both IP addresses belonged to Cogeco Cable and that they were leased to users in Hamilton, Ontario. The police sent a preservation demand to Cogeco, requesting that it preserve any subscriber information associated with the two IP addresses. Cogeco agreed to do so with regards to the second IP address, 67, but noted that the records for the first IP address, 79, were no longer on file.

[7] Detective Constable Jeremy Miller, a police officer since 2002, drafted an Information to Obtain ("ITO") for a general production order under s. 487.014 of the *Criminal Code*, R.S.C. 1985, c. C-46, which was granted on December 20, 2016. The affidavit appended to the ITO stated "that the information set out herein constitutes the grounds to suspect" that the subscriber(s) committed the offences of distribution and possession of child pornography, contrary to ss. 163.1(3) and 163.1(4) of the *Criminal Code* (emphasis added).

[8] Pursuant to the production order, Cogeco provided the subscriber information associated with the second IP address. The information revealed that the subscriber was Steve West, located at 46 Longwood Road, North, Hamilton. Further investigation confirmed that 46 Longwood was a residence, and that Steven Todd West was one of the owners.

[9] Using this information, the police sought a warrant to search the home for the following: electronic devices; stored data capable of being read by a computer; photographic film, digital images, and video; computer files or documents associated with Steven West or the “mikeandvikes” account; and any cellular telephones capable of accessing the Internet or storing images or video. The warrant was issued on February 7, 2017, authorizing a search on February 22, 2017.

[10] The search led to the seizure of digital devices and media, including a total of 19,687 files containing child pornography, and information showing that the appellant was the owner of the “mikeandvikes” Kik account. Of the files obtained, 10,804 were unique (i.e., not duplicates of other files). The files were found on five different devices: two laptop computers, two cell phones, and a USB drive.

[11] The appellant was subsequently arrested and charged with possession of child pornography, distribution of child pornography, and accessing child pornography, contrary to ss. 163.1(4), 163.1(3), and 163.1(4.1) of the *Criminal Code*.

[12] Prior to his trial, the appellant brought a *Charter* application, alleging that there were insufficient grounds for the issuance of both the production order and search warrant. The production of his subscriber information and the search of his

home were therefore invalid and constituted a breach of his rights under s. 8 of the *Charter*. He sought an order excluding all of the evidence pursuant to s. 24(2) of the *Charter*.

[13] The trial judge dismissed the application, finding no s. 8 breach. In arriving at this conclusion, he found that the information provided by Kik was "probably accurate" and that the search warrant ITO was comprehensive, reliable, reasonable, and sufficient to permit the issuance of the warrant. He also found that "sufficient information was presented to establish a reasonable suspicion permitting the issuance of the production order" (emphasis added).

[14] With the evidence admitted, the Crown's case was read in on consent and a finding of guilt was made against the appellant on each count.

[15] The appellant was sentenced to a global sentence of three years' imprisonment. The trial judge noted that while the appellant was a first-time offender and had expressed remorse and regret for his actions, he lacked insight into why he had committed the offences. The large number of files and disturbing nature of the images were aggravating factors. In light of the paramount principles of denunciation and deterrence, as well as the fact that the viewing and possession of child pornography perpetuates the violence enacted against children, a sentence of three years' imprisonment was deemed fit.

III. ISSUES ON APPEAL

[16] The appellant raises four issues on his conviction appeal:

(1) Was the production order validly issued?

(2) Was the search warrant validly issued?

(3) Was the failure of the police to include Kik's disclaimer about the lack of verification of the report information fatal to both ITOs?

(4) If the police breached the appellant's s. 8 rights, should the evidence be excluded pursuant to s. 24(2) of the *Charter*?

[17] The appellant also appeals his sentence on the basis that the trial judge failed to adequately consider the principle of parity. However, as I would allow the conviction appeal, there is no need to address this issue.

IV. ANALYSIS

(1) Was the production order validly issued?

[18] The appellant submits that the production order should not have been issued as the ITO used to obtain the order was predicated on the wrong legal test.

[19] Section 487.014 of the *Criminal Code* provides the authority under which a valid production order can be issued. It reads as follows:

> (1) Subject to sections 487.015 to 487.018, on *ex parte* application made by a peace officer or public officer, a justice or judge may order a person to produce a document that is a copy of a document that is in their

> possession or control when they receive the order, or to prepare and produce a document containing data that is in their possession or control at that time.
>
> Conditions for making order
>
> (2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to believe that
>
> (a) an offence has been or will be committed under this or any other Act of Parliament; and
>
> (b) the document or data is in the person's possession or control and will afford evidence respecting the commission of the commission of the offence. [Emphasis added.]

[20] Recently, in *R. v. Vice Media Canada Inc.*, 2017 ONCA 231, 137 O.R. (3d) 263, aff'd 2018 SCC 53, [2018] 3 S.C.R. 374, Doherty J.A. outlined the general principles governing the issuance of production orders. He stated, at para. 28:

> A production order under s. 487.014 of the *Criminal Code* is a means by which the police can obtain documents, including electronic documents, from individuals who are not under investigation. The section empowers the justice or judge to make a production order if satisfied, by the information placed before her, that there are reasonable grounds to believe that: (i) an offence has been or will be committed; (ii) the document or data is in the person's possession or control; and (iii) it will afford evidence of the commission of the named offence. If those three conditions exist, the justice or judge can exercise her discretion in favour of granting the production order. [Emphasis added.]

[21] In the case at bar, the affiant, Detective Constable Miller, swore the following in the affidavit to obtain the production order:

> I believe that the information set out herein constitutes the grounds to suspect that Cogeco Cable subscriber(s) with the internet protocol (IP) addresses of … [Emphasis added.]

[22] Detective Constable Miller misstated the standard another four times throughout his affidavit. He never asserted that he had evidence to satisfy the actual standard for the issuance of the production order – reasonable grounds to believe. Despite this clear flaw, the issuing justice authorized the production order.

[23] The error was also missed by the trial judge. In fact, the trial judge's conclusion for upholding the production order tracked the wording of the affiant, asserting that the ITO presented sufficient information to "establish a reasonable suspicion permitting the issuance of the production order." Beyond this clear error, the trial judge's reasons were also otherwise inadequate, as they provided no substantive analysis. The trial judge thus failed to properly carry out his role of determining whether the issuing justice could have concluded that the statutory threshold was met: *R. v. McNeill*, 2020 ONCA 313, at para. 30.

[24] In light of the error, no deference is owed to the trial judge's decision: *R. v. Cusick*, 2019 ONCA 524, 146 O.R. (3d) 678, at paras. 41, 100. Rather, it is now

this court's role to consider afresh whether there was a basis on which the production order could have issued.

[25] In my view, it was an error for the issuing justice to issue the order, given that the officer never subjectively asserted that he had the grounds necessary to satisfy the statutory requirements: *R. v. Storrey*, [1990] 1 S.C.R. 241, at pp. 250-251. There is no way to reasonably read the ITO and come away with any conclusion other than that there were reasonable grounds to suspect that an offence had been committed, that the information sought was in a person's control, and that the information would afford evidence of the commission of the offence. This is insufficient to permit the issuance of a production order.

[26] The production of the appellant's subscriber information thus amounted to an unauthorized search and a breach of his rights under s. 8 of the *Charter*: *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at paras. 66, 74.

(2) Was the search warrant validly issued?

[27] In light of my conclusion that the production order could not have issued, it is necessary to assess whether, if the information obtained pursuant to the production order is excised from the ITO for the search warrant, the warrant could still have been issued: *Spencer*, at para. 74; *R. v. Mahmood*, 2011 ONCA 693, 107 O.R. (3d) 641, at para. 116, leave to appeal refused, [2012] S.C.C.A. No. 111.

[28] In reviewing the ITO, it is clear that the warrant could not have been issued as, without the subscriber records, the police would not have been aware that the appellant was associated with the second IP address. Without this information, the police would not have been able to provide a location for the search or any details regarding the specific target. Under these circumstances, the statutory requirements under s. 487(1) could not have been met, as there would be no "building, receptacle or place" to search. The search of the appellant's home and electronic devices was therefore unlawful and a violation of the *Charter*: *Spencer*, at para. 74.

(3) Was the failure of the police to include Kik's disclaimer about the lack of verification of the report information fatal to both ITOs?

[29] Given my earlier findings, it is not necessary to address this issue.

(4) If the police breached the appellant's s. 8 rights, should the evidence be excluded pursuant to s. 24(2) of the *Charter*?

[30] The trial judge did not find a breach of s. 8 and, therefore, did not consider the question of whether the evidence obtained in violation of the appellant's *Charter* rights should be excluded under s. 24(2) of the *Charter*. In my view, the evidentiary record in this case is sufficient to permit this court to undertake the analysis: *R. v. Pilon*, 2018 ONCA 959, 144 O.R. (3d) 54, at para. 43; *R. v. Herta*, 2018 ONCA 927, 143 O.R. (3d) 721, at para. 60.

[31] The question is whether the admission of the evidence would bring the administration of justice into disrepute: *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353. In answering this question, the court must have regard to: 1) the seriousness of the *Charter*-infringing state conduct; 2) the impact of the breach on the *Charter*-protected interests of the accused; and 3) society's interest in the adjudication of the case on its merits: at para. 71.

[32] The first line of inquiry considers the seriousness of the *Charter* infringing conduct and whether it rises to a level of severity such that the courts should dissociate themselves from the conduct by excluding any evidence it produced: *Grant*, at para. 72; *R. v. Thompson*, 2020 ONCA 264, 62 C.R. (7th) 286, at para. 83. The courts should dissociate themselves from evidence obtained through a negligent breach of the *Charter*: *R. v. Le*, 2019 SCC 34, at para. 143.

[33] In this case, Detective Constable Miller was negligent in failing to apply the correct legal standard in his affidavit. The standard of reasonable grounds to believe, as outlined in s. 487.014 of the *Criminal Code* came into force on March 9, 2015: Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess., 41st Parl., 2013-2014 (assented to 9 December 2014). The production order in this case was signed on December 20, 2016, more than a year after the

amendments took effect. By this time, the requisite legal standard was well established and Detective Constable Miller should have been aware of this. This factor militates in favour of exclusion.

[34] The second line of inquiry under *Grant* "calls for an evaluation of the extent to which the breach actually undermined the interests protected by the right infringed": *Grant*, at para. 76. In the context of s. 8 of the *Charter*, the interests at issue are those of "privacy, and more broadly, human dignity": at para. 78. The seriousness of a breach resulting from an unreasonable search will reflect the level of privacy to which the individual was entitled to reasonably expect in the circumstances: at para. 78. Pursuant to the concept of discoverability, however, the impact of an illegal search on an individual's privacy and dignity will be lessened where the police could have demonstrated to a judicial officer that they had sufficient grounds to conduct a valid search: *R. v. Côté*, 2011 SCC 46, [2011] 3 S.C.R. 215, at para. 72.

[35] In this case, the impact on the accused's interests was serious. The police searched the appellant's subscriber information, his home, and his electronic devices. All of these areas attract a heightened expectation of privacy: *Spencer*, at paras. 66, 78; *R. v. Adler*, 2020 ONCA 246, 62 C.R. (7th) 254, at para. 33, citing

R. v. Silveira, [1995] 2 S.C.R. 297, at para. 140, and *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 2.

[36] The Crown, however, takes the position that, despite the error in the affidavit, the information available to the police, including the information contained in the Kik report, provided reasonable grounds to believe that a crime had been committed, that Cogeco had control of certain subscriber information, and that, that information would afford evidence of the commission of the crime. While this argument was put forward by the Crown on the first ground of appeal, it effectively amounts to an argument that the impact of the breach was lessened in light of the fact that the evidence was "discoverable", as the police had the requisite grounds to obtain the production order and, by extension, the search warrant.

[37] I do not accept this argument.

[38] The Kik report indicated that, at some unknown point between August 21, 2016 and September 19, 2016, a Samsung Model SM-T530NU was used to upload an image of child pornography as the profile picture to the "mikeandvikes" account. The report provided no information regarding the IP address associated with the upload. The only IP address information included was the first and last IP addresses to access the account. Cogeco subsequently indicated that the subscriber information associated with the first IP address was no longer on file.

In effect, then, the only information available was that the second IP address, which was associated with an Internet account (as opposed to a particular device), had accessed the Kik account on September 19, 2016, using an unknown device. Put differently, the only information the police had was that an unknown person, using an unknown device, had accessed the account from the 67 IP address on September 19, 2016.

[39] This was not a sufficient evidentiary basis to provide a "credibly-based probability" that the production of the subscriber information would afford evidence of the commission of the offence: *McNeill*, at para. 32. More was needed to establish a connection between the alleged offence and the subscriber information sought. Additional evidence was particularly important in this case, as it was not clear whether the IP address information provided could be relied upon, as the report stated that the IP address information collected "isn't verified by Kik." In his expert testimony, Martin Musters explained that further investigative techniques were available to the police, including requesting the precise IP address associated with the upload of the image, and inquiring as to the IP address associated with the email address used to register the account. These steps were readily available and may well have narrowed the focus of the investigation. In the absence of any evidence beyond the unconfirmed information that the Kik account had been accessed using a particular Internet account, the police were effectively

fishing for a connection to the offence. The appellant's subscriber information was thus not discoverable and the impact of the unlawful search on his *Charter*-protected interests was not diminished. This factor favours exclusion.

[40] Turning to the final line of inquiry, the court must determine "whether the truth-seeking function of the criminal trial process would be better served by admission of the evidence, or by its exclusion": *Grant*, at para. 79. In addressing this question, two relevant considerations are the reliability of the evidence obtained, and its importance to the Crown's case: at paras. 81, 83. In this case, the evidence is both reliable and critical to the Crown's case. This factor weighs in favour of admission.

[41] The final stage of the analysis under s. 24(2) involves balancing the factors under the three lines of inquiry to determine whether the admission of the evidence would bring the administration of justice into disrepute. While this balancing is not a mathematical exercise, where the first two inquiries militate in favour of exclusion, the third inquiry "will seldom, if ever, tip the balance in favour of admissibility": *R. v. Harrison*, 2009 SCC 34, [2009] 2 S.C.R. 494, at para. 36; *R. v. McSweeney*, 2020 ONCA 2, 384 C.C.C. (3d) 265, at para. 81; *Thompson*, at paras. 106-107.

[42] In this case, the first and second lines of inquiry provide a strong case for exclusion. The state conduct was negligent and it had a serious impact on the appellant's *Charter* rights. While this is a case where exclusion will gut the Crown's case, this result is appropriate. Admission of the evidence would bring the administration of justice into disrepute.

[43] For these reasons, the evidence obtained pursuant to both the production order and search warrant should be excluded under s. 24(2) of the *Charter*.

V. DISPOSITION

[44] In all the circumstances, I would allow the appeal and enter acquittals on all counts.

Released: "D.W." July 22, 2020

"M. Tulloch J.A."
"I agree. David Watt J.A."
"I agree. Gary Trotter J.A."