ONTARIO COURT OF JUSTICE

CITATION: *R. v. Owen*, 2017 ONCJ 729
DATE: 2017 11 03
COURT FILE No.: Brampton 15-4966

2017 ONCJ 729 (CanLII)

B E T W E E N :

HER MAJESTY THE QUEEN

— AND —

RICHARD OWEN

Before Justice M.M. Rahman
Reasons for Judgment on s. 8 Application, released on November 3, 2017

Maria Stevens..... counsel for the Crown
The applicant Richard Owen..... on his own behalf

RAHMAN J.:

I. Overview

[1] Peel Regional Police executed a search warrant at the applicant's home on April 22, 2015. They were looking for child pornography and seized several electronic devices from the home, including a computer tower containing hard drives.

[2] The applicant argued that the search of his home violated s. 8 of the *Charter*. His application took aim at two investigative orders – the search warrant for his home and a production order that preceded it. The applicant alleged many deficiencies with each order, including that each contained material misstatements or omissions and that each lacked reasonable grounds. The applicant also alleged that the manner of the search the police conducted on his home was unreasonable. In particular, he said that the police were guilty of an over seizure and that their search of the data on the computer that they seized was too intrusive. He sought exclusion of the evidence seized from his home.

[3] At the outset of the trial, I heard and granted an application by the applicant to exclude statements he made to the police.[1] The evidence heard in that *voir dire* applied only to that application. Subsequently, I heard evidence on this s. 8 application. Because of witness availability, the parties agreed that most of the evidence on the s. 8 *voir dire* would also apply to the trial. Also, it was understood that the applicant could use any findings from the statement application if this application required an analysis under s. 24(2) of the *Charter*.

[4] These reasons explain why I find that the applicant's s. 8 rights were violated and that the evidence should be excluded under s. 24(2) of the *Charter*.

II. Overview of the Investigation

[5] The investigation that led to the April 22, 2015 search of the applicant's home started on March 23, 2015. On that date, Cst. Chris MacDonald of the Peel Regional Police (PRP) Internet Child Exploitation (ICE) unit began investigating the suspected downloading of child pornography occurring on a peer to peer sharing network called Freenet.

[6] Cst. MacDonald parsed logs kept by a police database (known as the Internet Crimes Against Children (ICAC) database) and concluded that 80 child pornography files had been routed through IP address 24.212.213.252 (the suspect IP address) over the previous 240 days. He determined that three child pornography files had been downloaded by a computer at this IP address. The files had been downloaded on three separate days – December 7 and 15, 2014 and January 14, 2015. He could not otherwise say whether that the IP address had downloaded files on other days.

[7] Cst. MacDonald learned through a publicly available website that the suspect IP address was owned by an Internet Service Provide (ISP) called Teksavvy Solutions.

[8] On March 27, 2015, Cst. MacDonald served Teksavvy with a preservation demand under s. 487.012(1) of the *Criminal Code* requiring the ISP to retain its customer records for the suspect IP address as of March 27, 2015 at 3:40:59 a.m., GMT. That date and time was the most recent time that Freenet activity had been logged at that IP address. On March 31, 2015, Teksavvy confirmed that it had the records and would be preserving them for 21 days awaiting the service of a production order.

[9] On April 7, 2015, Cst. MacDonald applied for a production order for the suspect IP address. On April 8, 2015, a justice issued a production order directed at the Coordinator of Legal Affairs for Teksavvy Solutions.

[1] Those reasons are being released concurrently with these reasons.

2017 ONCJ 729 (CanLII)

[10] Teksavvy provided records for the suspect IP address on April 17, 2015. Those records said that the IP address was linked to an account in the applicant's father's name at 2650 Quill Crescent in Mississauga. The residence had been assigned the suspect IP address from February 7, 2015 until at least March 29, 2015.

[11] Further investigation revealed that the applicant and four other people lived in the home. The police also attended the applicant's address and discovered that the wireless signal that likely came from the home was secure, meaning it was password protected.

[12] Cst. MacDonald applied for a search warrant on April 20, 2015. It was granted the same day. Police executed the warrant on the morning of April 22, 2015 and seized several items including a desktop computer tower, a four-bay hard drive enclosure, laptop computers and other devices including an iPad and a mobile phone. They arrested the applicant and charged him with accessing and possession of child pornography.

III. Explanation of Freenet

[13] To understand the issues in this case, it is necessary to provide a brief explanation of how Freenet works. What follows is only a general explanation. More details about Freenet will be discussed below as they become relevant to the issues raised in the application.

[14] Freenet is a peer to peer network used for the storage and retrieval of files. It does not use central computer servers to store data. Rather, individual users may download Freenet software to their own computers to become part of the network. Once a user downloads Freenet software and goes online, that user's computer becomes a "node" on the Freenet network. The Freenet software creates dedicated space on the user's hard drive, known as a data store, for the storage of files.

[15] When a user wants to upload, or insert, a file on the network, the file is broken into many pieces, called blocks, and stored on other nodes in the network. These blocks are encrypted and sent randomly to a diverse group of nodes on the network. Those blocks then reside in the various nodes' data stores. A user who uploads the file has no way of knowing which other Freenet nodes store pieces of the file. Conversely, the other Freenet users who have pieces of the file stored on their hard drives have no way of knowing what kind of data they are storing on their own computers because the data is encrypted.

[16] When a user wants to retrieve or access a file from Freenet, the user must possess a unique identifier for that file, known as a manifest key. The manifest key is a long alpha-numeric string. To download a file, the user inputs the manifest key into Freenet's user interface and hits a download button. The user's computer then sends out requests for the file. Several requests are sent for any given file. Those

2017 ONCJ 729 (CanLII)

requests each contain a "split key" which is a unique identification key for one block of a file.

[17] The requests begin to travel the diverse network of nodes that make up Freenet, searching for blocks of the desired file. When a node receives a request, it checks its own data store to see if it has the block associated with the split key in the request. If the node does not have the requested block, it forwards the request to another Freenet node, which again checks its data store. The request is routed among various nodes until it finds a node that has the blocks. If a Freenet node has the requested block in its data store, it will send the requested block directly back to the Freenet node that requested it following the same path by which it received the request. Once the original requesting node has received all of its pieces, it will stop sending out requests for any pieces of the file.

[18] When a police officer wants to determine if a Freenet node is downloading child pornography, he parses the logs kept by the ICAC database. That database logs activity on Freenet from several law enforcement nodes operating on the network that have been modified for law enforcement use. In brief, it keeps track of blocks of known child pornography files passing through those law enforcement nodes.

[19] As mentioned above, a request for pieces of a file may travel through several nodes on its way to finding a node with pieces of a file. In other words, there might be many "innocent" nodes along the path of a request that are simply passing on the request to other nodes. The investigator's job is to determine which nodes are actually requesting the child pornography files, as opposed to simply re-routing them. The re-routing nodes are merely passing along a request and their users are not interested in downloading the file. Only the Freenet user at the requesting node wants to download the requested file.

[20] The criteria used by Cst. MacDonald to determine the identity of a requesting node was the subject of some dispute. I will discuss those criteria in more detail below as they relate to the applicant's various complaints.

[21] I will now turn to the various issues raised in the application to exclude evidence.

IV. Section 8 Issues: Sub-facial Attack

[22] I will consider the issues raised by the applicant in a slightly different order than he has set out in his application. I will first consider his sub-facial attacks on the ITOs because, if successful, they will result in excision of information. My review of the sufficiency of the ITOs must consider the ITOs, as amplified on review, with erroneous and unconstitutionally obtained information excised from them.

[23] The applicant argued that there are three areas where the affiant included either erroneous information, or failed to disclosure relevant information.

2017 ONCJ 729 (CanLII)

A. Fraudulent Statement in the ITOs

1 The Impugned Statement

[24] The applicant argued that one statement in the ITOs is so fraudulent that it engages this court's residual discretion to set aside the orders. The following statement appears in the ITOs for both investigative orders as part of the background information about how Freenet works:

> There is a counter on this process of repeated requests, which will decrease each time the request is past [sic] from node to node. The default number is 18, meaning the request should be past [sic] no more than 18 times before it stops looking for that piece.

[25] When he was cross-examined, the affiant acknowledged that this information was not complete. Freenet does use a counter. When a request is sent, it will not endlessly bounce around the network requesting pieces of a file. The request will only "hop" between nodes searching for the request a set number of times after which the request will expire. The number of times a request will bounce around among nodes is known as "hops to live." The default number of hops to live is set at 18. The affiant explained this much correctly in the ITO. However, he left out an important feature about how this counter works.

[26] As the affiant explained in cross-examination, when a Freenet connection is first established, the first node to which a request is sent randomly determines whether to have the counter decrement by one (to 17) or remain at 18. After that first "hop," the counter decrements normally by one for each "hop." This feature is meant to obscure the identity of the requesting node because it prevents an accurate backwards count to the requesting node by simply counting back the number of hops on the counter.

[27] When asked why he did not explain this feature of the software, the affiant said that, at the time he swore the ITOs, this feature "was not well known to the Freenet world" and so, for reasons of "investigative privilege," he purposely left it out. In response to a question from the court, the affiant said that he had received legal advice before deciding to omit this information.

2 Parties' Positions

[28] The applicant argued that because this statement is false, and because the affiant knew it was false when he swore to it, I should set aside the production order and the search warrant. He observed that at no point did the affiant voluntarily disclose this information and that it only came to light during cross-examination because of the applicant's own knowledge of Freenet and his careful review of disclosure.

2017 ONCJ 729 (CanLII)

[29] The Crown acknowledged the misstatement, but said that the affiant had no intention to mislead the issuing justice. Nor could the issuing justice have been misled. Ms Stevens said that the ITOs made clear that Freenet obfuscates the identity of the requesting node and that the affiant never asserted that he simply counted backwards to determine the identity of the requesting node.

2017 ONCJ 729 (CanLII)

3 Analysis

[30] In *R. v. Paryniuk*, the Court of Appeal recently affirmed that a trial court has a residual discretion to set aside an investigative order where "police conduct has subverted the pre-authorization process through deliberate non-disclosure, bad faith, deliberate deception, fraudulent misrepresentation or the like."[2] This residual discretion may be exercised even where sufficient grounds exist in the affidavit, after excising of the false statements.

[31] I am troubled by the affiant's failure to correctly describe how Freenet's counter worked. I accept that he had no intention to mislead the issuing justice. However, the statement quoted above was incorrect because it was incomplete. He knew it was incorrect when he included it. The misstatement only came to light during cross-examination by a self-represented accused.

[32] Moreover, the affiant's reason for omitting this information was wrong in law. Privileged information is routinely included in ITOs. Even police informer information, which is subject to a class privilege, is included in ITOs for the purpose of making full disclosure. The judicial officer reviewing the ITO is within the circle of privilege and any concerns about disclosure of privileged information are dealt with by sealing the ITO and then redacting the privileged information when the document is disclosed.[3] Omitting information that is relevant, even if it is privileged, is contrary to the requirement to make full, fair and frank disclosure.

[33] Further, this information was not subject to investigative privilege. Freenet was not created by or for law enforcement. The affiant was not even aware if Freenet's software is open source, meaning he had no way of knowing if anyone knowledgeable enough could learn of this little-known feature by examining the source code. In short, this was not information that was exclusively known to law enforcement, nor was the affiant certain that a sophisticated programmer could not discover it. Even if it had been appropriate to withhold information based on investigative privilege (and it was not), this information could not have qualified as such.

[34] I am unaware of the content of the legal advice the affiant received in deciding to omit this information. That information is privileged, and that privilege was not waived. I did not ask what the advice was. I was never made aware of it. The affiant either received correct legal advice and did not follow it, or he received

---

[2] *R. v. Paryniuk,* 2017 ONCA 87 at para. 69.

[3] See *R. v. Jaser* 2014 ONSC 6052 at paras. 65-67, where Code J. observed that attempting to protect an informer is not a reason to draft a paragraph in a misleading way.

incorrect legal advice and followed it thinking it was correct. I am inclined to believe it was the latter.

[35] However, even if I assume that he received bad advice, I can infer he would have received the advice from a Crown or police lawyer. In my view, the state cannot rely on its provision of patently wrong legal advice to suggest that the error was made in good faith. This was not a case where the affiant was seeking advice on an unsettled or changing area of the law. At best, this omission and the failure to correct it was negligent at an institutional level.

[36] Although any false statement and material omission from an ITO is serious, I cannot find that the impugned statement was "a subversion or corruption of the pre-authorization process." It was not essential to the overall understanding of the ITOs. As the Crown observed, at no point did the affiant suggest that merely counting backwards would reveal the identity of the requesting node. While it is true that including the correct information would have presented a more accurate picture of how Freenet anonymizes users, in the context of these ITOs, the misstatement did not subvert the pre-authorization process.

[37] Further, as mentioned above, the affiant did not intend to mislead the issuing justice. He did not include the information because he believed it was privileged. While that decision may have been wrong, it does not amount to a subversion of the prior authorization process. It does demonstrate carelessness and negligence (again most likely institutional, and not personal to the affiant) in the drafting and the pre-authorization process, a topic to which I will return later in these reasons.

[38] Finally, although the affiant did not correct this incorrect statement on his own, I cannot find that failed to do so for any subversive reason. I am satisfied that the affiant considered this paragraph to simply be background information that was not essential to his grounds. Although the affiant did consider hops to live as a disqualifying feature during his investigation, he did not rely on that criterion in the ITOs. I infer that it likely did not come to mind to correct this one paragraph in the ITOs and he was not trying to withhold information in order to thwart a successful challenge to the ITOs almost two years after they had been sworn.

[39] Because the passage about the counter is erroneous, it must be excised. However, as the applicant himself acknowledged, excising this information, on its own, would have little effect on whether there were sufficient grounds to issue the warrant.

B. Omitted information

[40] The affiant used four separate criteria to determine whether a node was a requester. In cross-examination, he testified that if any of these criteria were not satisfied it would disqualify the observed node as being a requester. The affiant also testified that he had been trained to analyze at least three files (as he did in this case) to reduce the likelihood of a false positive.

2017 ONCJ 729 (CanLII)

[41] The applicant argued that the affiant ought to have mentioned that all of these criteria had to be satisfied before he could conclude a node was a requester. He argued that this was a material omission because the issuing justice may have been misled by not being informed that all of the criteria needed to be satisfied. The applicant also argued that the affiant should have explained that he needed to analyze at least three files.

[42] Ms Stevens observed that the affiant did explain what investigative tool he used and what it was meant to determine. The ITOs state that investigators consider "many disqualifying factors" including a small number of requests proportionate to the size of a file. The ITOs also state that investigators will look for a volume of requests that is proportionate to the "number of nodes the node was connected to at the time" (known as even share, discussed below). Investigators will also look for "repeated and continuous requests for a specific file over a short period of time" as an indication that a Freenet user is a requester and not a re-router.

[43] I do not find that there was any material omission here. The affiant explained the criteria he looked for to determine whether a node was a requester and explained the basis for his conclusion that the suspect node was a requester. The fact that he did not explicitly say that the failure to meet any of the criteria would exclude the node as a requester could not have misled the issuing justice.

C. Erroneous Information

[44] The applicant argued that the ITOs contain erroneous information about how many data blocks make up a file and about the concept of "even share."

1 The Impugned Paragraphs

a) The Data Blocks Paragraph

[45] In his explanation about why he believed that the three particular files had been downloaded by the suspect, the affiant explained in the ITO what he had observed from his review of the logs. The following is his explanation about the file downloaded on December 15, 2014:

> ii. This database had had 132 pieces requested out of 606 total pieces of the file needed. Some of these are re-routing for other users, but I believe many are a direct result of a Freenet user, the suspect, downloading the file.
>
> [iii. contains the manifest key for the file]
>
> [iv. is blank]
>
> v. Volume of requests: I looked at the individual requests and there were no requests that looked to be not consistent with this node requesting the file. This is 132 pieces of the file, which is 21.78% of the

2017 ONCJ 729 (CanLII)

> file. I know this to be above the threshold needed to believe it is a requester.
>
> vi. Time: This download took 23 minutes to collect all of the pieces from the Freenet network. It started on the 15th of December 2014, at approximately 4:13 am (UTC) and finished at 4:37 am (UTC). I know this to be consistent with normal operation of a Freenet download.
>
> vii. There were also multiple instances that more than one request was coming in per second. This is consistent with this target node being a requester of the file, not re-routing a request.
>
> viii. Even share: This suspect Freenet node averaged 11.2 peers during the download time. The suspect node will try to evenly spread out the requests across these peers, which would be at approximately 54 requests each. In this case, there were 132 requests. This is consistent with this target being a requester, not re-routing.
>
> ix. Overall, I have analysed the Freenet logs in relation to this IP address and suspected child pornography file. **I believe that this IP address was requesting the file, not simply rerouting a request from a different Freenet user.** If that were the case, I would see less total requests in both quantity and even share. The time is also important, having multiple records coming in within a second. Re-routing has some processing time at each node and takes longer. [bold in the original]

[46] For each of the three downloaded files, the affiant referred to the foregoing criteria as support for his belief that the suspect IP address was requesting the files and not simply re-routing the files.

[47] In cross-examination, the affiant agreed that some of the numbers included above were incorrect. He arrived at this realization as the applicant took him through various documents, including ones that the affiant himself had used to form his conclusions. The applicant demonstrated that the file could potentially be re-constructed by two kinds of blocks or pieces – data blocks and check blocks. The affiant agreed that, taking into account check blocks, the total number of blocks that made up the file was 1,219, not 606. The affiant did not know the ratio of data blocks to check blocks that would make up a file. The affiant also did not know whether Freenet would first try to exhaust its search for all data blocks before looking for check blocks.

[48] The affiant then clarified that he meant 606 pieces of the file was the minimum number needed to recreate the file (because he referred in the ITOs to "the 606 total pieces of the file needed"). The affiant also agreed that the numbers in his paragraphs about "volume of requests" and "even share" were incorrect. Rather than the volume of requests equalling 21.78% of the file, it would have been about

2017 ONCJ 729 (CanLII)

half that amount. And rather than the even share number being 54 requests per peer, it would be 108 or 109.

[49] The affiant said that the changes in these numbers described above, would not have affected his conclusions. He explained that for volume of requests, 1% was the threshold required to believe that the node was requesting and not re-routing. Therefore, even 10% would be above that threshold. Similarly, he said that even with the change in the even share number (from 54 to 108 or 109), the number of requests (132) would still be above even share and therefore consistent with the node being a requester and not a re-router.

[50] The applicant did not go through each of the files, but the affiant agreed in re-examination that his calculations would be similarly off for each of the three downloaded files.

[51] The applicant testified on the *voir dire* and explained how Freenet requests work and how he had checked the affiant's calculations. He said that a requesting node would request all of the pieces of a file, not just the number required to re-create the file. In the above example, the requesting node would request all 1,219 blocks of the file. Therefore, if one were to observe every single request coming from the node, there would be a total of 1,219 requests. To re-create a file, at least half of the split key requests would have to be satisfied. The applicant testified that he performed an analysis on all three files and came to the same conclusion with each, that the numbers had been similarly miscalculated.[4]

b) The Even Share Paragraph

[52] The ITOs state that Freenet works off a principle called even share. The ITOs explained that a node tries to spread requests out as evenly as possible. The paragraph describing even share is set out below:

> The Freenet works off a principle called even share. A node will try to evenly spread out the requests they have among the nodes they are connected to at the time. For example, if the node has 10 peers and needs to find 100 pieces of the file, it will send approximately 10 requests per node. This is not exact; some could get 9 and others 11. This is referred to as even share. An investigator will look for a volume of requests that is proportionate to the number of nodes the node was connected to at the time. (emphasis added)

[53] In cross-examination, the affiant explained that he used even share as a threshold for determining if a particular node was a requester or simply a re-router. Even share was a general rule that the law enforcement community observed. He explained that if he observed anything below even share, it would disqualify the

[4] The applicant came up with these numbers by pasting the manifest keys for the three downloaded files into Freenet's Split Key File Explorer. He explained this both in his testimony and when he was cross-examining the affiant.

2017 ONCJ 729 (CanLII)

node as a requester. Anything at even share or above would qualify the node as a requester. He also testified that even share is "not an exact science" and that it would be possible to have multiples of eight times even share.

2 Parties' Positions

[54] The applicant argued that the following should be excised from the ITOs:

- references to the "total number of pieces" for each file;
- the subsection about "volume of requests;" and
- the subsection on "even share."

[55] The applicant said that the court should be concerned that the affiant did not seem to understand the way Freenet works and had not conducted the same review that the applicant himself did to determine the correct number of blocks which made up the files. He said that the affiant's testimony demonstrated that he did not know how Freenet software chooses which peer to send a request to and therefore he could not have (subjectively) known whether evenness was a factor in determining that a node was a requester.

[56] The applicant also argued that the affiant's explanation of even share is problematic. He said that the affiant described even share as a "functional mechanic" in the ITOs, but that in cross-examination he described it as a minimal threshold to determine if a node was a requester. He said that the erroneous numbers are cause for concern because they contradict the affiant's assertion that Freenet uses even share, because the number of observed requests in the ITO far exceeds even share by over a factor of two. He said that the affiant did nothing to explain this large discrepancy, and why the number of requests far exceeds even share. The applicant alleged that the affiant misled the issuing justice by suggesting that even share, which was observed under controlled conditions, was a core element of the software's operation, even though the affiant himself testified he had observed requests that far exceeded even share.

[57] The applicant argued that the Crown cannot rely on amplification to correct this error because the correct information was not known to the affiant at the time he swore the ITO. The applicant said that the affiant could have corroborated the information on his own, in the same manner the applicant did. The affiant's choice not to do so meant that he ran the risk of including incorrect information.

[58] Ms Stevens acknowledged that the affiant's information about the total number of blocks was incorrect. However, she said that the error can be remedied by amplification. She argued that this is a technical point and that "the affiant performed a mathematical equation using a number he now has learned should not have been used." More importantly, the error did not affect the affiant's ultimate conclusion because, even with the correct information, the number of blocks downloaded was over the threshold he was using. Again, she urged the court to consider the amplified record because knowledge of the required threshold is a

2017 ONCJ 729 (CanLII)

technical point that is required to understand the consequence of the affiant's calculation error.

3 Analysis

[59] I agree with the applicant that the erroneous information about a file's total number of blocks cannot be corrected through amplification, because the affiant was not aware of it at the time he swore the information. The affiant only learned of his mistake when the applicant took him through spreadsheets during cross-examination. Amplification is only available to correct minor and technical errors with information known to the police at the time the warrant was obtained.[5] If the Crown were permitted to amplify erroneous information based on information learned after obtaining the warrant, it would undermine the prior authorization process.[6]

[60] Further, this is not a minor or technical error. The information is "technical" in the sense that it involves specialized knowledge. But it is not a technical error as described in the amplification cases, such as *R. v. Araujo*.[7] The calculation here was integral to the affiant's conclusion about whether a node was a requester or a re-router. The affiant did not just transpose a few numbers or make a mistake in addition. He made a mistake based on a fundamental misunderstanding about how to calculate these numbers. He used those numbers to either qualify or disqualify a node as a downloader. Therefore, the erroneous numbers were neither minor nor technical errors and cannot be corrected by amplification.

[61] The affiant deposed in the ITO that he was looking for even share. However, the numbers he included showed an amount well over even share. This may have left an impression that his conclusion was stronger than it was. This is especially problematic because the affiant did not explain anything about the thresholds he used. In fact, the ITOs state that the applicant was expecting to see even share, not a number that far exceeded it.

[62] The next question is how much of the erroneous information should be excised.

[63] I agree with the applicant that the subsections about volume of requests and even share should be excised. The calculations in those paragraphs are wrong. The affiant ought to have known they were wrong. I cannot simply substitute the correct numbers into those paragraphs, because they were not known to the affiant at the time.

[64] I do not agree that the total number of requests should be excised because the ITOs do not say that the file was made up of a total of 606 pieces but that 606 pieces would be required to re-create the file. That statement remains correct.

---

[5] *R. v. Ting*, 2016 ONCA 57 at para. 70.
[6] *R. v. Morelli*, 2010 SCC 8 at paras. 42-43.
[7] *R. v. Araujo*, 2000 SCC 65.

2017 ONCJ 729 (CanLII)

[65] I am not convinced that I should excise the affiant's entire conclusion. The affiant testified that, even with the correct information, he would have reached the same conclusion because it was above the threshold he was using to determine if a node was a requester. In other words, even if I excise the incorrect numbers, his conclusion would have remained the same.

[66] Even with this information excised, and even if the same information is excised from all of the three downloaded files, there is still ample information to find that the files had in fact been downloaded and that the node was a requester and not simply a re-router.

2017 ONCJ 729 (CanLII)

V. Section 8 Facial Attack: Lack of Reasonable Grounds in the ITOs

[67] The most significant defect that the applicant alleged was the lack of reasonable grounds to believe that the production order and the search warrant would yield the evidence they sought. In a nutshell, the applicant said that there was no nexus between the downloading of child pornography that the affiant observed and the IP address of the node that requested the files. The applicant argued that both the production order and the search warrant suffer from this defect.

A. The Production Order

[68] The affiant deposed that he believed the suspect IP address had downloaded child pornography on at least three occasions. The production order in this case sought records relating to that specific IP address. Specifically, the production order required the ISP to produce the following:

> Copies of all documents, including the customer name and address as well as computer logs, usage records, and other business and operating records relating to the use of the computer system(s), by individuals to access the Internet through accounts at Teksavvy Solutions, while assigned the Internet protocol address 24.212.213.252 on 3/27/2015 3:40:59.

[69] The ITO states in Appendix B that there were reasonable grounds to believe that the offences of possessing and accessing child pornography had been committed in a one-month period preceding March 2015 in Brampton, Ontario. The affiant testified that the appendix ought to have alleged that the offences were committed in a four-month period preceding March 2015 and that the location should have been Mississauga, Ontario.

1 Parties' Positions

[70] The applicant argued that the ITO makes no connection between March 27, 2015 and the offences described in the ITO. Specifically, he said that the affiant only confirmed that three child pornography files had been downloaded by the

suspect IP address on December 7 and 15, 2014, and January 14, 2015. Other than those three dates, the ITO did not otherwise fix particular dates when the suspect IP address downloaded illegal files. Rather, it stated that it 80 such files were "associated to" that address in the preceding 240 days, but that it was not a requester for all of them.

> I noticed some activity with the IP address 24.212.213.252. This led me to display only suspected child pornography records from 24.212.213.252 over the last 240 days and had more than 50 records. From here I learned the following:
>
> > There were 80 unique files of suspected child pornography listed as associated to this IP. However, I know from my analysis that this IP was not necessarily the requester for all of these entries. Some of these instances reflect instances when the IP was simply re-routing the requests for other users, as per the normal network functionality. Other instances were indicative of requestor activity as follows:

[71] The affiant then listed the three occasions where he observed the suspect IP address showing requester activity on December 7, and 15, 2014 and January 14, 2015. He did not list any more instances, nor did he specify a time frame within the 240 days in which other requester activity had occurred.

[72] The applicant argued that, because the ITO listed the last requester activity associated with the suspect IP address as occurring on January 14, 2015, there were no grounds to believe that records associated with that IP address on March 27, 2015 would afford evidence of the offences. He said that the ITO would have had to establish reasonable grounds that the subscriber on March 27 was the same as the subscriber on one of the three days child pornography was downloaded.

[73] The applicant relied on the following paragraph in the ITOs that explains what an IP address is, and how it is assigned to a subscriber:

> Internet Protocol Address (IP Address) – is a unique address that devices use in order to identify and communicate with each other on a computer network utilizing the internet protocol standard. An IP address will have a standard form that is represented as: four numbers, from 0-255, separated by periods; for example, an IP address could be 123.45.67.89. Any participating network device – including routers, computers, time-servers, printers, Internet fax machines, and some telephones – can have their own unique address. An IP address can be thought of as the equivalent of a street address or phone number for a computer or other network device on the Internet. Just as each address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. <u>It should also be noted that IP</u>

2017 ONCJ 729 (CanLII)

> addresses are not permanent fixtures for a given user. Some Internet service providers use dynamic IP addresses, meaning that periodically their assigned IP address will be reassigned to another user who requires it to access the Internet, and they will be assigned a new IP address. Depending on the Internet Service Provider, a user may keep the same IP address for months, or have several IP addresses in a day. ISPs' typically keep logs of IP assignments for a limited time period, police can use these logs to identify an address and potential user associated to suspected criminal activity observed online at a particular moment in time. [emphasis added]

[74] The applicant argued that, because IP addresses can be re-assigned by ISPs from one subscriber to another, there was no basis to believe that the subscriber who downloaded child pornography in December and January was the subscriber attached to that account on March 27, 2015. Without that basis, the production order should not have issued.

[75] The Crown argued that the pre-conditions for issuing a production order were met here. Ms Stevens said that it was open to the issuing justice to infer that the same Freenet node that downloaded files in December and January was still operating on March 27, 2015. She said this could be inferred based on the assertion that the IP address had logged over 80 unique child pornography files over the last 240 days, and that Freenet activity was observed from that IP address on March 27, 2015.

2 Analysis

[76] A judge reviewing an investigative order, like a production order or a search warrant, works "within a narrow jurisdictional compass."[8] The reviewing judge does not engage in a *de novo* review of ITO in support of the order. Rather the reviewing judge considers the record, as amplified on review, and determines whether the investigative order *could* have issued.

[77] An issuing justice may draw reasonable inferences from the evidence set out in an ITO. The affiant is not required to underline the obvious, nor is the affiant required to negative every innocent inference that may arise from the facts. The standard of reasonable grounds requires only a credibly-based probability, and not a *prima facie* case or proof on a balance of probabilities. The issuing justice's finding that there are grounds must be "based on the operation of reason and not mere suspicion."[9]

[78] Section 478.014 authorizes the issuance of a production order if there are reasonable grounds to believe that the following two pre-conditions in s. 487.014(2) have been met:

[8] *R. v. Ebanks,* 2009 ONCA 851 at para. 20.
[9] *R. v. Campbell*, 2010 ONCA 588 at para 54.

2017 ONCJ 729 (CanLII)

(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 offence.

[79] The applicant's argument about the lack of nexus between March 27 and the offences is really an argument that the second pre-condition has not been met. His submission is that there were no reasonable grounds to believe that the ISP records would afford evidence respecting the commission of the offence.

[80] The question here is – could the issuing justice have found a credibly-based probability that Teksavvy's records for a subscriber on March 27, 2015 would afford evidence respecting the commission of the offences of possession or accessing child pornography?

[81] In my view, there was no basis for the issuing justice to find that there were reasonable grounds that Teksavvy's records would afford evidence respecting the offence.

[82] The grounds to believe that Teksavvy had records that would afford evidence of the offence can be summarized as follows:

(1) This IP address had 80 child pornography files associated to it in the 240 days preceding March 23, 2015. Not all of those files had been requested by this address. A number of those files may have simply been relayed through the address.

(2) On December 7 and 15, 2014 and January 14, 2015, the suspect IP address downloaded child pornography files.

(3) Freenet activity was logged at this IP address on March 27, 2015.

(4) IP addresses are like a street address. They are unique addresses which identify devices on a computer network.

(5) IP addresses are not permanent fixtures. Depending on the ISP, an internet account may be assigned an IP address for months or have several IP addresses in a day.

(6) ISPs maintain logs of IP assignments which can be used to identify an address and potential user associated to suspected criminal activity observed online at a particular moment in time.

(7) Teksavvy does not keep internet usage records beyond 30 days.

[83] The ITO had to establish a credibly-based probability that subscriber records as of March 27, 2015 would afford evidence respecting the commission of an offence.

2017 ONCJ 729 (CanLII)

The offences here occurred in December 2014 and January 2015. I agree with the applicant that it would have been speculative to draw a connection between the subscriber on March 27 and the subscribers in December and January. Therefore, there was no basis for the issuing justice to conclude that there were reasonable grounds to believe the records would afford evidence of the offences. I say that for the following reasons.

2017 ONCJ 729 (CanLII)

[84] First, the ITO states that IP addresses can change many times over a short time period, depending on the ISP. There is nothing in the ITO to suggest that Teksavvy assigned its subscribers their IP addresses for certain periods of time. The fact that an IP address could change as many as several times in one day meant that there was only a possibility, not a probability, that the subscriber assigned was assigned the suspect IP address.

[85] Second, the ITO states that Teksavvy did not keep records past 30 days. A plain reading of that assertion would mean that any records in Teksavvy's possession would only go back as far as February 27.[10] The records would not go back as far as January 14, 2015, the last date that the affiant observed child pornography being downloaded.

[86] Finally, the affiant's assertion that 80 suspected child pornography files were associated with this IP address in the 240 days preceding March 23 also did not assist in establishing reasonable grounds. The ITO said that not all of those 80 files had been requested by a node at that address. More importantly, it did not specify a time frame in which the IP address had requested or even re-routed those 80 files. In fact, the overview to the affiant's analysis of the Freenet logs said that "I extracted information about three files from the logs, [and] formed the belief that these files were being requested by this IP address." In the summary of his analysis, the affiant said "I know that a computer utilizing Teksavvy Solutions IP addresses is operating the Freenet software and "deduced from the Freenet requests made by this node, I believe that this user downloaded at least three files." The clear implication of this statement is that the affiant is concerned with the three downloaded files he believed had been requested by the suspect IP address. Indeed, in his testimony on the *voir dire*, the affiant made it clear that the offences he was investigating involved the three downloads in December and January.

[87] I cannot accept the Crown's submission that the issuing justice could have inferred that Freenet activity on March 27, 2015 was from the same Freenet user operating in December and January. The only information in the ITO supporting the conclusion that it was the same user, was the affiant's implicit assertion that it was the same node, when he referred to it as "*this* node" (my emphasis). Without more information about why the affiant believed it to be the same node, the issuing justice would have been speculating that the same subscriber was using the same Freenet node throughout.

[10] As mentioned above, as it happened Teksavvy was able to tie the IP address to a particular subscriber as far back at February 7, 2015.

[88] The affiant's testimony about why he believed the node that had downloaded child pornography in December and January was the same node that was operating from the IP address on March 27, 2015 was telling in this regard.

[89] When asked why he believed it was the same user, he said he relied on two facts to draw that inference. First, he explained that, in his experience, Freenet was not very common in Brampton and Mississauga. Second, he said that the node had shown "continuous activity" throughout. The applicant conceded that neither of these two facts were in the ITO. The affiant acknowledged in his testimony that it was those two facts that led him to believe that the user on March 27 was the same user who had downloaded the child pornography. While the affiant's view is obviously not determinative (if the ITO otherwise provided a basis for that belief) it speaks to the inferential gap that existed in the ITO, because it is the opinion of the very person who stated he had reasonable grounds.

[90] Statements of belief are different than statements of fact. The issuing justice must be capable of assessing the reasonableness of the belief on the basis of the record. In this case, the issuing justice was not armed with that information. The affiant did not include the two main reasons for his belief. The record before the issuing justice was not capable of supporting the inference outside of the affiant's mere assertion that it was the same node.

[91] Justices may draw on their own life experience to draw inferences about well-known, everyday situations. Not so with the workings of sophisticated computer software. Information about computers, and the way computer networks operate, requires specialized knowledge. To draw inferences about this very technical area, a justice must be armed with more information than might be required for a common situation where the inferential gap might be filled with through common knowledge.

[92] Finally, I am mindful that the phrase "affords evidence" must be given a broad interpretation. That phrase embraces evidence that may lead to other evidence after further investigation.[11] However, in the context of this ITO, the evidence the affiant was seeking was the location of the offence. The affiant deposed that "[w]ith the results of the Production Order, I expect to have the physical location of the offence revealed" and "[p]olice wish to have the Internet Service Provider produce documents necessary to continue the investigation by revealing the physical location of the offence." Although the affiant said that further investigation would be necessary, that statement was made in the context of determining the person responsible for the offence, rather than the location at which it was committed.

[11] *CanadianOxy Chemicals v. A.G. Canada*, [1999] 1 SCR 743.

2017 ONCJ 729 (CanLII)

3 Conclusion

[93] The production order ITO did not provide a basis to find reasonable grounds to believe that the records being sought would afford evidence of the offence. Consequently, the production order must be set aside.

[94] The production order provided the applicant's home address. Without the subscriber information obtained as a result of the production order, there would have been no basis in the search warrant to search the applicant's home. The result is that the search warrant must also be set aside.

[95] If I am wrong in setting aside the production order, I will consider whether there was a basis for the search warrant to have issued, assuming the production order was otherwise valid.

2017 ONCJ 729 (CanLII)

B. The Search Warrant

[96] The applicant's argument that the search warrant is invalid is similar to his argument about the production order.

[97] The applicant said that the last time the affiant had seen a file downloaded was on January 14, 2015. Teksavvy's records could only connect the suspect IP address to the applicant's physical address from February 7 to March 29, 2015. As with the production order, the fact that IP addresses could be re-assigned was the prominent feature of the applicant's attack. Again, relying on the ITO's explanation that IP addresses are not fixed, and can change frequently, the applicant said there was no link between the commission of the offence and the address in question. Therefore, there was no basis to believe that the child pornography files had been downloaded by the subscriber at 2650 Quill Crescent.

[98] The question raised by the applicant's complaint is – could the issuing justice have found a credibly-based probability that the items to be searched for would be found in the applicant's home? In my view, as with the production order, the answer to that question is no and I find that the search warrant must be set aside.

[99] The search warrant ITO established that the applicant's father was the subscriber for the suspect IP address from February 7, 2015 onwards. While it did not rule out that he had the suspect IP address before February 7, 2015, there was nothing in the ITO that would have established a credibly-based probability that it was the same in that earlier period.

[100] The affiant's grounds to believe that a computer used at 2650 Quill Crescent downloaded child pornography can be summarized as follows:

> (1) This IP address had 80 child pornography files associated to it in the 240 days preceding March 23, 2015. Not all of those files had been requested

by this address. A number of those files may have simply been relayed through the address.

(2) On December 7 and 15, 2014 and January 14, 2015, the suspect IP address downloaded child pornography files.

(3) The suspect IP address was assigned to Neal Owen at 2650 Quill Crescent from February 7, 2015 to at least March 29, 2015.

(4) IP addresses are like a street address. They are unique addresses which identify devices on a computer network.

(5) IP addresses are not permanent fixtures. Depending on the ISP, an internet account may be assigned an IP address for months or have several IP addresses in a day.

(6) ISPs maintain logs of IP assignments which can be used to identify an address and potential user associated to suspected criminal activity observed online at a particular moment in time.

[101] I do not accept the Crown's argument that the issuing justice could have inferred that, because the IP address had been the same from February 7 to at least March 29, Teksavvy likely assigned IP addresses for longer periods of time. The ITO did not arm the issuing justice with sufficient information to draw this conclusion. Indeed, it gave the issuing justice the opposite information. The paragraph explaining how IP addresses work did not explicitly say that there were two different kinds of ISPs – those that assigned addresses for long periods of time and others that changed their assignment frequently. The paragraph said that police could use logs of subscriber activity "to identify an address and potential user associated to suspected criminal activity observed online at a particular moment in time." (emphasis added)

[102] Further, I do not accept the Crown's submission that the issuing justice could have inferred that, because there was Freenet activity at the IP address in the 240 days before March 23, that it was the same Freenet user who downloaded the files in December and January. Unlike the production order, the ITO did not state that there was Freenet activity at the suspect IP address on March 27. There is no time period mentioned when in the 240 days prior to March 23 that the child pornography files moved through the suspect IP address. Indeed, the search warrant ITO does not actually say that Freenet activity was still occurring as of March 23. It simply says that the affiant parsed logs on March 23 that went back 240 days.

[103] Moreover, as with the production order, I find it telling that, in cross-examination, the affiant stated that he believed that it was the same Freenet user because Freenet was not that commonly used in Mississauga and Brampton, and because he observed continuous activity. That information, which was the basis for

2017 ONCJ 729 (CanLII)

his belief that it was the same node, was not included in the ITO. Again, that information might have filled the missing inferential gap.

[104] The only way to tie internet activity to a physical address is with evidence that the IP address at which the activity took place was being used at a particular place, at a particular moment in time. In cross-examination, the affiant characterized the likelihood that the subscriber whom he observed downloading child pornography being different from the subscriber whose information he obtained from Teksavvy as a "technical speculative possibility." I cannot accept that characterization on this record. Given the dynamic nature of IP address assignment, there was a very real probability that the subscribers were different. While the affiant may have concluded otherwise based on his knowledge of how uncommon Freenet was in Peel Region, he did not share that information with the issuing justice.

[105] The following analogy illustrates the problem with the warrant for the applicant's home. If the police received information that a suspect was staying in a short-term rental building on January 14 and the police had information that rentals in the building spanned from a few days to several months, the police would have to take some steps to confirm that the suspect (or someone matching his description) still lived in the apartment on March 27 before they could obtain a warrant to enter that place and arrest the suspect. Without that information, it would be speculation to believe that the suspect was still staying in the place.

[106] Despite my conclusions that both investigative orders must be set aside, I will still consider the applicant's remaining s. 8 complaints because they are relevant to any analysis under s. 24(2).

C. Unsourced Material

[107] The applicant complained that the affiant did not explain the source for his assertion about the average number of Freenet peers the alleged requesting node had.

[108] I agree with the Crown that this information was in fact sourced. The affiant referred to having analyzed logs created by the ICAC database. He explained how law enforcement nodes on Freenet observed activity and that this information is logged in the ICAC database. The affiant did not fail to source this material, and the analogy the applicant drew to unsourced hearsay is misplaced.

D. Incorrect Target of Production Order

[109] The applicant argued that the production order is invalid on its face because it was directed at the "Coordinator, Legal Affairs, Teksavvy Solutions." He said that the production order ought to have been directed at the company and not an individual person working at the company. He pointed to the affidavit that the Coordinator of Legal Affairs sent back to the police to support this submission. In

2017 ONCJ 729 (CanLII)

that affidavit, the Coordinator said that she did not have possession or control of the documents, but that she realized that the intent of the production order was to obtain documents from her employer. The Coordinator further deposed that she had taken the production order to her employer who then authorized the production of the requested documents.

[110] The applicant relied the British Columbia Supreme Court decision of *R. v. Sullivan*[12] in support of his argument. In that case, Mr. Sullivan, a Telus employee, sought an exemption from complying with a production order. Mr. Sullivan supervised employees at Telus who were responsible for receiving and replying to production orders. The issuing justice believed that a production order had to be directed at a natural person rather than a corporation. On the exemption application, Mr. Sullivan deposed that, because of the terms of his employment and the confidential nature of Telus' data, could not deal with Telus' records without the company's authority.

[111] It appears that, through his exemption application, Mr. Sullivan was trying to stop police from directing production orders his way. It was in that context that Hyslop J. made the following comment upon which the applicant bases his argument:

> 26 Lastly, when a document is in the possession of a company or owned by a company, it would be wrong for the police to apply for, and those who grant the production orders, to expect an employee to take the data and documents that they are not authorized to do by their employer.

[112] I have no evidence before me that the Teksavvy's Coordinator of Legal Affairs could not access data or was unwilling to accept responsibility for making sure her employer complied with the production order. The fact is, as an employee of the company, she did provide the documents, albeit with the technical qualification that she did not possess the documents.

[113] Accepting the applicant's argument would allow form to triumph over substance. I do not accept the Coordinator of Legal Affairs' overly technical interpretation of the production order. The clear intent of the production order, as she herself acknowledged, was that the corporation produce its records. There is no question that the production order named the Coordinator of Legal Affairs for Teksavvy because that is the person who would be responsible for responding to the request. The fact that the co-ordinator could obtain the records at Teksavvy and provide them to the police is evidence that she was the correct person to whom the production order should be directed.

E. Production Order's Incorrect Description of Offences

[114] The applicant argued that the production order does not properly describe the offences for which evidence is sought.

---

[12] *R. v. Sullivan*, 2009 BCSC 1769.

2017 ONCJ 729 (CanLII)

1 Description of the Offences

[115] Appendix B to the production order describes two offences – possession and accessing child pornography. It alleges that the offences were committed by an unknown person or persons of Brampton, Ontario, "on or about a one month period last past and ending March 2015."

[116] In his evidence on the *voir dire*, the affiant explained that he made a mistake in Appendix B. He said the time period should have been four months and the place should have been Mississauga. He acknowledged that Appendix B was wrong in its description of the offence.

[117] In Appendix B to the search warrant, the affiant described the offence as having occurred "over a two month period last past and ending on or about February 2015."

[118] In cross-examination, while acknowledging the error, the affiant said that he put more information in Appendix B than required, and that he knew of many search warrants that simply listed the crime and the *Criminal Code* section number. He testified that he did not think he had to describe the offence as accurately as in an information charging an offence.

[119] When asked about the discrepancy between the time period in Appendix B to the production order and Appendix B to the search warrant, the affiant expressed uncertainty about why he used two different time periods:

> Q. Why does that differ from Appendix B on the search warrant?
>
> A. As for the two month saying over the – just the span of it, I'm not quite sure why I went with different dates there, February over a two month period versus March over a four.
>
> Q. So you're just not sure why you did that?
>
> A. Yeah, 'cause the time period for the indictment later is going to be more tied to when we have all the evidence. This, as you know, we only had three uploads [sic] and Freenet activity so the main information that I wanted to put in here was that it was what I believe to be possession of child pornography, to wit, child – sorry, graphic computer files and accessing.

2 Parties' Positions

[120] The applicant argued that the offences for which Teksavvy's records are being sought occurred in December 2014 and January 2015. There is no evidence that any offences occurred in the one month preceding March 2015 (i.e. February 2015).

2017 ONCJ 729 (CanLII)

[121] Ms Stevens acknowledged that the affiant made a mistake but said that it can be corrected through amplification. She said the error is a minor, administrative one capable of being cured through amplification.

3 Analysis

[122] The description of the offence being investigated in a search warrant must be sufficient to reasonably inform the person in charge of the premises the nature of the offence and the object of the search.[13] In the production order context, the description should be such that it permits the order's target to discern the scope of the order. The failure to properly identify an offence in the warrant is potentially fatal to the warrant and may render it facially invalid.

[123] I find the affiant's inability to explain why he used different times periods in the production order and the search warrant, and his explanation that he meant to use a four-month period prior to March 2015, curious. The offences he identified were the same for each order. Why would he describe them differently in each? Further, four months prior to March would have included the month of November, a month in which no files had been downloaded. On his own evidence, he meant to refer to downloads that occurred in December and January.

[124] Nonetheless, I accept the affiant's explanation that he made a mistake and I agree with the Crown that this error can be correct by way of amplification. This was an administrative error made by the affiant. The information was known to him at the time and it is a minor error. In any case, the target of the production order would not have been misled by the error.

F. The "*Branton* Error"

[125] The applicant argued that the search warrant is facially invalid because the face of the search warrant included language suggesting that the evidence was being sought in respect of the "suspected commission or intended commission" of an offence.

1 The Defect

[126] The face of the search warrant says that it authorizes police to search for certain things listed in Appendix A "that being [sic] sought as evidence in respect to the commission, suspected commission, or intended commission of an offence" against the *Criminal Code*.

[127] In the search warrant ITO, the affiant deposed that he had reasonable and probable grounds to believe, and did believe, that certain items would be found at 2650 Quill Crescent.

[13] *R. v. PSI Mind Development Institute Ltd*. (1977), 37 C.C.C. (2d) 263 (Ont. H.C.) at p. 268.

2017 ONCJ 729 (CanLII)

[128] The ITO does not specifically say which subsection of s. 487 under which the affiant is applying for the warrant. Similarly, the warrant does not specifically say which subsection of s. 487 that the issuing justice granted it under.

2 Parties' Positions

[129] The applicant argued that the inclusion of the words "suspected commission or intended commission" rendered the search warrant facially invalid. In addition to *R. v. Branton*,[14] he relied on the recent decision in *R. v. Kramshoj*.[15] In *Kramshoj*, Healey J. held that the *Branton* error rendered the warrant facially invalid.

[130] Ms Stevens urged me to follow *R. v. Nurse*.[16] In *Nurse*, Coroza J. held that, although a search warrant contained a *Branton* error, there was no possibility of confusion by the issuing justice or the officers executing the warrant about the scope of the search.

3 Analysis

[131] It is no doubt important that search warrants, as judicial orders, be accurate. They ought not to authorize a search broader than is requested or permitted. The search warrant here was on an outdated form. The impugned language ought not to have been included. Having said that, it is important to consider what actually happened here.

[132] The affiant deposed that he had reasonable grounds to believe an offence had been committed. There is no question that the issuing justice issued the warrant on that basis, and not based on the suspected or intended commission of an offence. Moreover, it is apparent from Appendix B to the search warrant that the offences for which evidence was being sought occurred in the past. I agree with the approach taken by Coroza J. in *Nurse*, and I find that nobody could have been misled about what the warrant authorized.

[133] Even if I had found the impugned phrase to have been improperly included, I would follow the approach taken by Fairburn J. (as she then was) in *R. v. Nguyen* and sever those words from the warrant.[17]

G. Appendix A to the Search Warrant and Overbreadth

[134] The applicant argued that Appendix A to the search warrant, which lists items to be seized, is overbroad.[18]

---

[14] *R. v. Branton*, 2001 CanLII 8535.
[15] *R. v. Kramshoj*, 2017 ONSC 2951.
[16] *R. v. Nurse*, 2014 ONSC 1779.
[17] *R. v. Nguyen,* 2017 ONSC 1341 at para. 116. See also *R. v. Sonne*, 2012 ONSC 584.
[18] The applicant originally argued that Appendix A was overbroad only because of its inclusion of item #4, printed child pornography material. After I had received written submissions, I asked the parties to make submissions on whether all of Appendix A was overbroad. I asked for those submissions because the applicant may not have appreciated that his failure to argue that the list was overbroad was potentially fatal to his argument that the police were guilty of over seizure.

2017 ONCJ 729 (CanLII)

1 The Appendix

[135] I begin by noting that Appendix A to the search warrant is identical to Appendix A to the ITO. One would expect that the list of items would be the same. However, the entire page of Appendix A to the ITO has been cut and pasted to form part of Appendix A of the search warrant. The header to the search warrant's Appendix A says the following:

> This Appendix 'A' forms part of the Information to Obtain a Search Warrant application under Section 487 of the Criminal Code for the search of a dwelling house located at 2650 Quill Crescent, Mississauga, ON. [emphasis added]

[136] The appendix then contains the title "Appendix 'A'" with the words "Items Being Sought" in parentheses below it. The list of items is then prefaced with the following language that clearly belongs in an ITO and not an investigative order:

> THE INFORMANT SAYS THAT he has reasonable and probable grounds to believe and does believe that there are certain things to wit:

[137] The list of items to be seized follows the foregoing statement of reasonable grounds. The list is set out in its entirety below:

> (1) Any computer system, as defined by 342.1(2) of the Criminal Code, capable of accessing the internet, but not limited to, desktop computers, and netbook computers. And all auxiliary items necessary for the proper operation of the system; including but not limited to cables, power adaptors, monitors, modems, routers, software and operational manuals.
>
> (2) Any data storage device or media capable of holding data, as defined by 342.1(2) of the Criminal Code; including, but not limited to, DVDs, CDs, hard-drives, and memory sticks.
>
> (3) Any written memory aids containing computer passwords, including, but not limited to, memos, sticky notes, address books and notepads.
>
> (4) Any printed material believed to contain Child Pornography, including, but not limited to, magazines, printed stories or pictures.
>
> (5) Any documentation pertaining to the occupants of the location to be searched that will assist in proving their occupation of the location and control of the computer equipment located therein, including, but not limited to, rental agreements, utility bills and mail.

[138] After this list of items, the appendix contains terms and conditions for the search of any computer system that is seized. The police were entitled to search for data involving the two offences listed in Appendix B, including images and videos on the devices or at a remote storage location, and associated files that might be

2017 ONCJ 729 (CanLII)

evidence of knowledge and control. The police were also entitled to search for data that would provide evidence of "use, ownership, access and configuration" of the devices.

2 Parties' Positions

[139] The applicant argued that this list is overbroad. He said that the warrant permitted the wholesale seizure of all electronic devices in this house and "provided the seizing officers with no meaningful way of separating the wheat from the chaff." He argued that the warrant ought to have limited the police to searching for and seizing computers running Freenet, rather than any computer in the house that could connect to the internet. The applicant also argued that there was no basis in the ITO to include item #4, printed material, because the ITO was silent about why printed material would be in the home.

[140] Finally, the applicant argued that the terms and conditions in the warrant permitting the search of the computer are overbroad. He said that there was no basis to grant authorization to search for anything more than the three video files the affiant believed had been downloaded in December and January.

[141] Ms Stevens argued that the list is reasonable and supported by the grounds in the ITO. She said that the ITO supports the inclusion of item #4 because it says that pictures and movies are highly portable and can be moved from computer to computer including to external media. She observed that printed child pornography would be illegal and subject to seizure anyway. Finally, regarding the search of the computers, Ms Stevens noted that in *R. v. Vu*,[19] the Supreme Court did not require the inclusion of detailed search protocols and that the terms and conditions here struck the right balance between minimizing invasion of privacy and discovering evidence.

3 Analysis

[142] Before dealing with the substance of the claim, I should comment on the form of Appendix A. The cutting and pasting of Appendix A from the ITO to Appendix A of the search warrant demonstrates a degree of carelessness. I am aware that documents like this are created from precedents and that mistakes are made while cutting and pasting. However, a search warrant is a judicial order and must appear on its face to be a judicial order. It must be presented to the occupants of the place being search upon request. The occupants must be able to examine the warrant to determine if it is a valid order, and whether it authorizes the police to invade their privacy. There should be no ambiguity whether the appendix to an order belongs with it, or with some other document. Nonetheless, I agree with the applicant that this carelessness does not affect the facial validity of the warrant.[20]

---

[19] *R. v. Vu*, 2013 SCC 60.

[20] I had raised this issue with the parties at the same time I had asked for further submissions about the overbreadth of Appendix A. The applicant chose not to make submissions on the issue.

2017 ONCJ 729 (CanLII)

[143] On the issue of overbreadth, I am not convinced that the entirety of Appendix A is overbroad. There were grounds to believe that the items listed in the appendix, with one exception, would be found in the place. For each of the items, the ITO established a basis for believing that the items would be found in the place. Although the inclusion of the words "including but not limited to" should be avoided because they may be seen as delegating identification of items to the police[21], in this case I find that it does not render the list overbroad. If the items listed after that phrase were excluded, the police would still have had the authority to seize the items described generally before that phrase.[22]

[144] I also cannot accept the applicant's argument that the police should only have been permitted to search for the three files they believed had been downloaded. The ITO sets out the affiant's experience about the portability of electronic files and that they might be moved to different computers or to other storage media. That information provided a basis for items #1 and #2.

[145] Moreover, the ITO explained that it would be impossible to restrict forensic analysis to specific times and dates, because not every file and activity undertaken by a computer is time and date stamped. The ITO also stated that forensic analysis would look for other information that would be useful in revealing the identity of the computer's user. That evidence was not contradicted or undermined during the *voir dire*. This warrant did not authorize a fishing expedition. It reasonably circumscribed the police's authority to search for evidence of the offences listed in the warrant.

[146] The one exception in Appendix A is item #4. I agree with the applicant that there were no grounds in the ITO to believe that any printed materials were in the house. The only mention of printed material within the ITO was the following paragraph:

> Non-electronic evidence <u>will be searched for</u> at the scene, such as printed child pornographic materials, either from the user or purchased and brought to this location. This will be seized and used as evidence towards the offences listed on appendix B. [emphasis added]

[147] There are two problems with the foregoing paragraph. First, it does not provide a basis to believe that the particular item – printed child pornography materials – will be found in the place to be searched. This is not a case like *R. v. Vu*, where the issuing justice could have drawn the common sense inference that printed materials would be found in the place. I also cannot accept Ms Stevens' argument that when the affiant was referring to "external media" that he was referring to printed material. It is apparent from the context that he was referring

[21] The words "namely" or "specifically" should be substituted for that phrase so that these are not open categories.

[22] Although the categories may seem broad, I note that in *R. v. Vu,* 2011 BCCA 536, aff'd (without reference to this specific point), 2013 SCC 60 (*Vu (BCCA)*), did not consider the phrase "documentation identifying ownership and/or occupancy of the property" to be impermissibly vague.

2017 ONCJ 729 (CanLII)

to electronic storage media. The above-quoted paragraph about printed material reinforces that view.

[148] Second, and more importantly, the paragraph demonstrates a fundamental misunderstanding of the nature and purpose of a search warrant. Rather than informing the issuing justice of the reason for believing that the particular things would be found in the place to be searched, it simply tells the issuing justice that the police plan to look for this item and, if found, use it as evidence.

[149] Although a search warrant is an investigative tool, it is not meant to be an exploratory order. The list of items to be seized in a search warrant is not a wish list. A search warrant may be more accurately described as a seizure warrant. It authorizes police to enter a place and seize those items listed in it. Items may only be listed in the warrant if there are reasonable grounds to believe they will be found in the place to be searched. The order is called a search warrant not because it is a blank cheque to search for anything related to the offence being investigated, but because it permits the police to search for those items listed in the warrant.

[150] Subject to s. 489 of the *Criminal Code*, and the plain view doctrine, the list of items to be seized not only limits what the police can seize, but acts to limit the scope of their search once in the place. For example, if the police obtain a search warrant authorizing them to enter a home and seize only a five-foot tall statue, they would be exceeding their search authority by opening kitchen drawers and cupboards that would be too small to conceal the item.[23] Moreover, once the police find the item(s) listed in the warrant, they no longer have any reason to remain in the place for search purposes. They would be exceeding their authority if they remained in the place or continued to search for items related to the offence after seizing all the items listed in the warrant.

[151] Indeed, in addition to his testimony on the *voir dire* (about collecting evidence of printed material), the wording of the items in Appendix A to the ITO suggests that the affiant misconstrued the nature of a search warrant. Appendix A to the ITO is supposed to list items that the police have reasonable grounds to believe are *certain things in* the place to be searched. In listing the items in the ITO that he believed were in the place, he preceded each item with the word "any." The inclusion of the word "any" is problematic because it does not suggest that the affiant believed that those items would be found in the place. Rather, it suggests that the affiant was seeking authority to enter the home and then seize "any" such items that he found. Because there was a basis for inclusion of each of these items, I cannot find that the mere inclusion of the word "any" before them in the ITO renders the warrant defective. I mention it because it informs the lack of any basis for item #4 and its inclusion in the warrant.

[23] See *Vu (BCCA)*, *supra*, at para. 47. American courts refer to this as the "elephant in the matchbox" doctrine because a warrant authorizing police to search for an elephant would not authorize them to look in a matchbox.

2017 ONCJ 729 (CanLII)

[152] Even though item #4 ought not to have been included, that does not mean the search warrant is invalid. Where part of an investigative order is defective, it does not necessarily render the entire order invalid. A reviewing court may sever the offending portion of the warrant if there is a clear line of demarcation between it and the valid part of the warrant, and where nothing was seized under the authority of the bad provision.[24] This is such a case. I also note that item #4 did not expand the scope of the search because the police were properly entitled to seize other documentary evidence.

[153] Item #4 can be severed from the search warrant; its inclusion had little effect since no printed material was seized.

VI. Reasonableness of the Search

A. Over seizure of Items

[154] The applicant argued that the police seized too many items and conducted the search in a "dragnet fashion." He said that the police ought to have circumscribed their seizure based on the information contained in the ITO and not simply relied on the appendix to the warrant listing the items to be seized.

[155] The Crown counters that the police did not seize anything outside of the items listed in Appendix A and therefore did not engage in an impermissible over seizure.

[156] I agree with the Crown that the police did not engage in an over seizure. The police did not seize any items outside of the items listed in Appendix A. Because I have found that Appendix A was not overbroad, I cannot find that there was an unconstitutional over seizure. The police were not required to limit their search base on the information in the ITO. If anything, courts have disapproved of reliance on the ITO as a means of limiting the scope of the search. The searching officers must look to the list of items to be seized in the warrant as their guide. They are not required to look any further, and in many cases they will never have read the ITO. The search here was conducted within the limits imposed by Appendix A.

B. Overbroad Search of the Computer

[157] The applicant argued that the search of the computer seized from his home was overbroad. He said that the police ought not to have been allowed to "perform a systematic file-by-file search of every picture and video on the computer."

[158] The Crown argued that the search here was not overbroad. Ms Stevens said that the affiant clearly set out in the ITO how the search of any seized computers would be conducted and that Appendix A to the warrant had terms and conditions that would limit the categories of data that would be searched for during the analysis.

[24] *Grabowski v. The Queen*, [1985] 2 S.C.R. 434.

2017 ONCJ 729 (CanLII)

[159] I agree with the Crown's position that the police did not stray outside of the terms of the warrant in their search of the computers. While it is true that computer searches may yield private information unrelated to the criminal investigation, it is also true that files can be hidden in a way that masks what they are. Moreover, the police cannot be limited in looking only for the files that they observed had been downloaded. The ITO provided a basis for the issuing justice to believe that there would be more child pornography than the three files which were downloaded. I find nothing improper about the forensic search of the computer here. Indeed, I accept the evidence of Cst. MacDonald, Cst. Kral, and Cst. Jenkins, that the search was done in a manner that attempted to minimize the intrusiveness of the search.

2017 ONCJ 729 (CanLII)

VII. Section 24(2) of the *Charter*

[160] Having found that the production order and search warrant should be set aside, I must go on to determine whether the evidence should be excluded under s. 24(2) of the *Charter*.

A. Seriousness of the Breach

[161] The first step of the *R. v. Grant*[25] inquiry requires a court to examine how serious the police conduct is that led to the breach of an applicant's *Charter* rights. This conduct can be placed on a continuum with good faith, technical breaches on one end, and bad faith, flagrant breaches on the other. A court may also consider whether the breach in issue is part of a pattern of *Charter* breaches.

[162] Although I have determined that the production order and search warrant in this case ought not to have been issued, the search was not warrantless. The police conducted the searches here relying on what they believed was a valid warrant. An independent judicial officer authorized them. As Fish J. remarked in *R. v. Morelli*, the searches here was unwarranted but not warrantless.[26] Apart from the misstatement about the counter, the ITO was not misleading in any way. There are no examples of the affiant intentionally misleading the issuing justice.

[163] There are two more areas to consider under the seriousness of the breach. The first is the police's approach to the prior authorization process. The second is the other *Charter* breaches that I have found in the statement application.

[164] As I have explained above, the police's conduct here demonstrates carelessness towards the prior authorization process. I am mindful that police officers are not expected to be experts at legal drafting and that even sloppy drafting does not require setting aside a warrant or a finding of bad faith. However, the problems that I have identified above demonstrates a careless attitude to the prior authorization process. Those errors are as follows:

---

[25] *R. v. Grant*, 2009 SCC 32.
[26] *R. v. Morelli*, 2010 SCC 8 at para. 99.

(1) The affiant's misstatement about the hops to live counter.

(2) The affiant's incorrect calculation, and lack of knowledge of the number of pieces making up a file.

(3) The use of an out-dated search warrant form with language that has been found on other occasions to render a warrant invalid.

(4) The use of an appendix to the search warrant that identified it as belonging to the ITO.

(5) The inclusion of printed materials in the list of items to be seized, despite the absence of any grounds to believe such material would be found in the place, and based on the apparent belief that the police were merely entitled to search for such items once in the place.

[165] Negligence, carelessness, or inattention to constitutional standards in obtaining the warrant can "tip the scales in favour of exclusion" even where there is no impropriety or bad faith.[27] Although the foregoing problems did not by themselves, result in breaches of s. 8, in my view they remain relevant to the seriousness of the breaches that did occur because they are directly related to police's conduct in the prior authorization process.

[166] Moreover, the additional *Charter* breaches committed by police must factor in to the seriousness analysis. The police breached the applicant's rights under ss. 9, 10(a) and 10(b) of the *Charter*. As I have found, those breaches were the result of a negligent and careless attitude towards the occupants of the home being searched. A breach will be more serious where there are multiple breaches that demonstrates a pattern of police misconduct, or abuse of the accused's *Charter* rights. Although the conduct of the police in this case did not demonstrate a flagrant or wilful disregard of the applicant's *Charter* rights, it did demonstrate negligence. The cumulative effect of the breaches here renders the breach of the applicant's s. 8 *Charter* rights more serious.

[167] I find that the first step of the *Grant* inquiry favour exclusion.

B. Impact on the Applicant's *Charter*-Protected Interests

[168] The second step in the *Grant* inquiry requires a court to consider the impact of the breach on the applicant's *Charter*-protected interests. Where s. 8 is concerned, the greater the invasion of privacy, the more serious the breach will be.

[169] The breach in this case had a very significant impact on the applicant's *Charter*-protected interests. Not only was the warrant in this case for a dwelling – a place which attracts the highest degree of privacy – but it allowed for the search of

[27] *R. v. Rocha*, 2012 ONCA 707 at para. 43.

2017 ONCJ 729 (CanLII)

computers and other electronic media. As Fish J. observed in *Morelli*, the search of one's home and personal computer is among the most intrusive:

> it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer. Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.[28]

[170] Because of the intrusiveness of the breach, this step of the *Grant* inquiry favours exclusion.

C. Society's Interest in Adjudication on the Merits

[171] The third step of the *Grant* inquiry clearly weighs in favour of admitting the evidence. The evidence is reliable and essential to the Crown's case. However, as Doherty J.A. observed in *R. v. McGuffie*, where the first and second steps of the *Grant* inquiry favour exclusion, the third step will seldom, if ever, tip the balance in favour of admission.[29]

[172] In this case, when considering all three stages of the *Grant* analysis, admitting the evidence would bring the administration of justice into disrepute. The breach here was serious and had a significant impact on the applicant's *Charter*-protected interests. Despite the reliability of the evidence and its importance to the Crown's case, the long-term repute of the administration of justice is best served by exclusion.

VIII. Conclusion

[173] The applicant's s. 8 *Charter* rights were violated and the admission of that evidence would bring the administration of justice into disrepute. Consequently, the application to exclude evidence seized from the applicant's home is granted.

Released: November 3, 2017

Justice M.M. Rahman

[28] *R. v. Morelli*, at para. 105.
[29] *R. v. McGuffie*, 2016 ONCA 365 at para. 63.

2017 ONCJ 729 (CanLII)