HEARING BY A MILITARY JUDGE

Citation: *R. v. McGoey*, 2014 CM 3020

Date: 20141017

Preliminary Proceedings

Asticou Courtroom
Gatineau, Quebec, Canada

Between:

Her Majesty the Queen, Respondent

- and -

Private J. McGoey, Applicant

Before: Lieutenant-Colonel L.-V. d'Auteuil, M.J.

REASONS FOR THE APPLICATION ON DISCLOSURE

(Orally)

[1] Private McGoey is charged with four offences related to child pornography, and more specifically for offences punishable pursuant to section 130 of the *National Defence Act* for accessing, possessing and making available child pornography, contrary to subsections 163.1 (3), (4) and (4.1) of the *Criminal Code*.

[2] Those offences would have allegedly occurred between March and June 2013 at or near Canadian Forces Base Borden. The charge sheet is dated 28 May 2014 and charges were preferred on 2 June 2014. A court martial has not been convened yet.

[3] As set out at section 187 of the *National Defence Act*, at any time after a charge has been preferred but before the commencement of the trial, any question, matter or objection in respect of the charge may, on application, be heard and determined by a military judge when the court martial has not been convened yet.

[4] Accordingly, Lieutenant-Commander Walden, on behalf of the applicant, Private McGoey, filed a notice of application about an issue involving disclosure, which was received by the Court Martial Administrator on 9 September 2014.

[5] On 25 September 2014, I was assigned by the Chief Military Judge to hear the application filed by Private McGoey and, on the same day, a pre-trial hearing conference took place on the phone where I determined, with the agreement of both parties, that the matter would be heard at the Asticou courtroom on 8 October 2014 at 9:30 a.m.

[6] Then, on 8 October 2014, I proceeded with the hearing on this matter. During the hearing, the parties filed a number of documents in order to substantiate their respective positions, which included three affidavits with a number of exhibits attached to them, and the information to obtain (ITO) a search warrant dated 12 June 2013. Also, Special Constable Versace testified on behalf of the respondent.

[7] First, the context in which this matter about disclosure has been raised by the applicant must be summarized. The Ontario Provincial Police (OPP) has a Child Sexual Exploitation Unit which conducts specific investigations regarding those involved in the possession and access to child pornography material on computers and on the Internet.

[8] One of the activities of this unit is to monitor electronic networks known for being used by people in order to possess and access child pornography. It allows the unit to gather information for tracking down those who are involved in such criminal activity. One of these networks is the Ares network, which is an open source public file-sharing network.

[9] Without being too technical, it is important to understand that on this type of network, a file may be divided in different segments among multiple users and be reassembled from different sources. Further to a search, a list of files and descriptive information about them will be provided, and by clicking on a search result, a user will download the file from multiple users having different segments of it.

[10] Keeping this description in mind, it is easy to conclude that a user on the Ares network then becomes a host computer in order to share files with other users on that network. However, such a user may have the ability to configure or reconfigure the settings of the Ares software on his or her computer in order to decide what type of file he or she will allow to be downloaded on his or her shared directory.

[11] When the download of a file is initiated, a list is created about the information and the Internet Protocol (IP) addresses of computers, having confirmed that they have the same file or portion of the file. Such a list provides an opportunity to detect and investigate computers involved in sharing files with child pornography.

[12] Special Constable Versace is a member of the OPP and he is the co-author of an automated investigative tool for the Ares network, which is the Roundup Ares program. It is an investigative tool created internally and that has been shared with some other law enforcement organizations around the world.

[13] The program is able to download suspected child pornography files from a suspect IP address previously identified without being recognized. It then allows

investigative authorities to confirm the exact nature of the material downloaded and provide them with information for further investigation.

[14] According to the ITO produced at the hearing, a police officer from the Child Sexual Exploitation Unit used the software program Roundup Ares and it provided information concerning a specific IP address. It was learned that a different child pornography file was downloaded on the same computer on three different days, which are 28, 29 and 30 May 2013. The computer at this IP address was associated with some other investigative files identified since 6 March 2013 in the Internet Crime Against Children (ICAC) database.

[15] The exact nature of the three movie files downloaded was confirmed by the investigator as being child pornography material. The IP address was identified as registered to Rogers Communications, which confirmed the exact identity of the subscriber.

[16] On 4 June 2013, OPP officers met and informed Canadian Forces National Investigation Service (CFNIS) officers located in Borden of the current investigation about a person residing in a building on the base. It was decided that the CFNIS Borden detachment would assume investigative responsibility and lay charges if required.

[17] On 12 June 2013, a search warrant was executed at that building and the accused's computer was seized.

[18] Corporal Flinn, a member of the CFNIS, conducted a forensic examination of the accused's computer, using a digital forensic software tool named Internet Evidence Finder (IEF) in order to locate and identify the presence of child pornography material, which he did, and he accordingly prepared his report on this investigation.

[19] As previously mentioned, the charge sheet was signed by a Director of Military Prosecutions' representative on 28 May 2014 and the four charges on the charge sheet were preferred on 2 June 2014. Initial disclosure was received by defence counsel's office on 11 June 2014.

[20] Lieutenant-Commander Walden was also invited to communicate with CFNIS Borden detachment in order to get two compact discs containing additional information not provided with the initial disclosure. Essentially, those discs had on them:

(a) Corporal Flinn's curriculum vitae and forensic report; and

(b) an unaltered copy of the accused's hard disk drive (HDD).

[21] On 20 June 2014, a "will say" statement was produced by the prosecution.

[22] On 12 August 2014, Lieutenant-Commander Walden requested further disclosure, which was a copy of the software Roundup Ares, and a copy of the investigative folder and files of interest. In reply, the prosecution told him that it would not provide such copy

of the software and the investigative folder and files of interest, but could arrange for the defence counsel and his expert to use the software Roundup Ares at an OPP detachment.

[23] Between mid-July and end of August 2014, various exchanges took place between the CFNIS organization and the defence counsel concerning access and control by the defence counsel of the additional information on the two discs, without any success as of this day. Mainly, the issue is how the control of the information would be performed by the defence counsel. It seems that the latter and the police have a disagreement on this matter.

[24] During the hearing, I was told by the respondent that the investigative folder and files of interest were on the two discs, being part of the forensic report. Also, a sworn copy of the ITO was finally disclosed to the defence counsel by the prosecution.

[25] The applicant told me that regarding the disclosure of Corporal Flinn's curriculum vitae, the forensic report and the accused's hard disk drive, the only issues are the method of passing to him those elements and the parameters about the control he should exercise on them, especially the forensic report and the HDD, considering the very sensitive nature of the material and the fact that he would like to make a copy of it for practical reasons, including passing it to an expert. Also, he claimed that the manner imposed by prosecution to disclose this evidence would have him reveal the name of the expert he retained, which would be contrary to any practice known.

[26] Concerning the disclosure of the software program Roundup Ares, the applicant submitted that it is necessary to have it, in order to understand clearly how information was obtained to substantiate the ITO, and allowing him to potentially challenge the validity of the search warrant that led to the search and seizure of the accused's computer where it is alleged that child pornography material has been found. For the exact same reason, the applicant considered that the digital forensic software tool named Internet Evidence Finder should be disclosed because it was used by CFNIS investigators to identify child pornography material on the accused's computer.

[27] The respondent does not see any issue with Corporal Flinn's curriculum vitae. It is clearly not an issue. However, concerning the forensic report and the accused's hard disk drive, he said that the approach taken by the prosecution is the following one; considering the sensitive and serious nature of the material disclosed, no copy can be made by the defence counsel in order to submit it to an expert and the only way for the latter to get one is directly from the prosecution once identified by the defence counsel. Essentially, the respondent took the position that the manner that such things must be disclosed should be set judicially instead of doing it on agreement between parties.

[28] About the software program Roundup Ares, the respondent took the position that no copy of it would be disclosed. He based his position on two grounds: first, it is beyond the control of the prosecution because the OPP internal methods of investigation are not under the control of the military prosecution; second, there is a common law public interest privilege applicable in the circumstances that would justify the prosecution to not disclose such an internal method of investigation which is used by the OPP for this type

of crime. However, despite his position, he clearly told me that he saw no issue in providing to the defence counsel, and/or the accused's expert, access to the program at an OPP location to allow an examination of it.

[29] Finally, regarding the digital forensic software tool named Internet Evidence Finder, the respondent submitted that it is a software on the market that any expert should be able to identify and use without any problem, which is a situation not requiring the respondent to provide a copy of it.

[30] It appears to me that the general issue raised by the application is more about the method for disclosure of the evidence than what has to be disclosed or not. The right to disclosure is not an end in itself. Its purpose is to help ensure a defendant's right to fundamental justice with its dual issues of reliability of the result and fairness.

[31] It is well settled law that the prosecution has a duty, a legal duty, to disclose all relevant information to the accused, not merely the material that the prosecution intends to use as part of its case. The fruits of the investigation that are in its possession are not the property of the prosecution to secure a conviction, but the property of the public to ensure that justice is done.

[32] The prosecution is, however, granted some discretion related to relevance and privilege. In that context, there is no obligation on the prosecution to disclose or produce documentation it doesn't have. This is an ongoing obligation imposed on the prosecution, and it must disclose any new information or material to the defence as soon as it comes into its possession or control.

[33] The right of the accused to disclosure of information exists whenever there is a reasonable possibility of the information being useful to the accused in making full answer and defence. This right is protected under section 7 of the *Charter* and helps to guarantee the accused's ability to exercise the right to make full answer and defence as this was recognized by the Supreme Court of Canada in *R. v. Carosella* (1997), 112 C.C.C. (3d) 289, at paragraph 37 of the decision.

[34] It is trite law that the purpose of the prosecution of offences is not to secure a conviction at all costs; it is to lay before a court what the prosecution considers to be credible and relevant evidence that would establish the commission of an alleged offence. The prosecution has the duty to present all available evidence firmly, thoroughly, but fairly. The prosecution does not win; the prosecution does not lose.

[35] The connections between the duty to disclose and the duties of the prosecutor were expressed by Justice Claire L'Heureux-Dubé, as she then was, in *R. v. O'Connor* (1995), 103 C.C.C. (3d) 1, and at page 50 of that decision, at paragraph 101, she states:

> Though the obligation on the Crown to disclose has found renewed vigour since the advent of the *Charter*, in particular s. 7, this obligation is not contingent upon there first being established any violation of the *Charter*. Rather, full and fair disclosure is a fundamental aspect of the Crown's duty to

> serve the court as a faithful public agent, entrusted not with winning or losing trials but rather with seeing that justice is served: *Stinchcombe, supra,* at p. 7

[36] The prosecution's exercise of its discretion is reviewable by a military judge. The absolute withholding of information relevant to the defence can only be justified on the basis of a legal privilege. This privilege is reviewable on the ground that it is not a reasonable limit on the right to make full answer and defence in a particular case.

[37] This is not a case in which the prosecution is attempting to keep information from the defence. The prosecution was and is always prepared to disclose everything that is under its control and in the hands of both police organizations, and to provide access to that material. What is in dispute is the manner in which access should be provided. I accept that the prosecution's insistence on making disclosure in a specific way is rooted in a sincere and honest concern that child pornography might inadvertently be disseminated.

[38] About the disclosure of Corporal Flinn's curriculum vitae, I understand that it is of no concern and it must be disclosed as soon as practicable.

[39] Concerning the forensic report, which includes the investigative folder and files of interest, and the accused's hard disk drive, the issue, from the respondent's perspective, is the potential dissemination of child pornography material.

[40] I would say that in the same manner as the prosecutor is required to be ethical in the conduct of the trial and providing disclosure, defence counsel has consistently shown the same as a matter of ethics. I do not have any reason to distrust defence counsel, from that perspective, that he will not disseminate this material beyond the scope of his personal control or possession from time to time. I do see that the same thing should apply to the expert chosen by the defence counsel.

[41] Then, the conditions suggested by defence counsel as an undertaking in his email dated 16 July 2014 appear to me as more than reasonable in the circumstances and I do not see any reason in this case to go beyond or afar from them. Those conditions should have been considered sufficient by the prosecution in order to meet its obligation concerning disclosure.

[42] About the disclosure of the software program Roundup Ares, I do find relevant for the accused to know, in relation to the charges preferred, how information was gathered in order to substantiate the ITO that led to the search and seizure of his computer, and obtained for supporting some essential elements of the second and fourth charge on the charge sheet.

[43] However, on the other hand, I do understand the respondent's concern about the dissemination of a particular investigative technique which is represented by using the software program Roundup Ares. Mr. Versace was quite clear in his testimony that the software program was established by law enforcement authorities for internal use only and that it is obviously part of an investigative technique to detect those involved in the possession of and access to child pornography material.

[44] In those circumstances, I find that prosecution's proposal to provide access to the applicant by allowing the defence counsel and/or his expert to attend at the OPP premises and, in privacy, examine the software program and talk to those who created it and are using it, would put the prosecution in a position as having met its disclosure obligation on this specific issue. This suggestion is reasonable in the circumstances and considering my conclusion on this issue, I do not see the need for me to consider the application of a common law public interest privilege as raised by the respondent.

[45] Finally, concerning the disclosure of a copy of the digital forensic software tool named Internet Evidence Finder, the respondent put to the Court that a forensic expert meeting present day industry standards would be proficient with IEF, and indeed possess the software such as to afford the defence access to the data without the need for a copy of it.

[46] Concerning this specific matter, this affirmation appears to be reasonable in the circumstances. According to Corporal Flinn's evidence, IEF is a product developed by the industry to recover data on hard drives and in the live memory of computer devices. It is a licensed product and presumably cannot be shared.

[47] I would say that in these circumstances, I think that the prosecution must disclose information about the exact version of IEF used by the CFNIS investigator. Then, if, for any reason, the forensic expert retained by defence counsel is not proficient with IEF or does not possess such software, the prosecution, through the CFNIS organization, would have to provide access to the applicant by allowing the defence counsel and/or his expert to attend at the CFNIS premises and, in privacy, apply the software program to the applicant's copy of the hard drive.

FOR THESE REASONS, I:

[48] **GRANT,** in part, the application;

[49] **ORDER** the disclosure of Corporal Flinn's curriculum vitae to the applicant's defence counsel as soon as practicable;

[50] **ORDER** that the forensic report, which includes the investigative folder and files of interest, and the accused's hard disk drive, be disclosed by the prosecution to the applicant's defence counsel on signature by the latter of the following undertaking:

(a) That he only makes one copy of any material containing child pornography to the hard drive of a laptop designated by DDCS for that purpose and that such a copy be deleted from its location on the hard drive and the recycle bin within the same time limit as undertaking 2.

(b) That all original discs will be returned to ITCU or the prosecutor within 45 days of completion of trial. In the event an appeal is made, the original discs may be retained until 45 days after completion of that process.

(c) That the report with images will only be viewed by defence counsel, any experts retained by defence counsel, and the accused for the purpose of court martial proceedings. The accused shall not be provided possession or unaccompanied access to the images or report.

(d) And that any expert retained by defence counsel undertakes to not make any copies of any materials containing child pornography and follow undertakings 2 and 3.

[51] **ORDER** that the prosecution provides access to the applicant by allowing his defence counsel and/or his expert to attend at the OPP premises and, in privacy, examine the software program Roundup Ares and talk to those who created it and are using it.

[52] **ORDER** that particulars be provided to the applicant's defence counsel concerning the version used by CFNIS investigators of the digital forensic software tool named Internet Evidence Finder on the accused's hard drive computer and if, for any reason, the forensic expert retained by defence counsel is not proficient with the IEF or does not possess such software, the prosecution, through the CFNIS organization, would have to provide access to the applicant by allowing the defence counsel and/or his expert to attend at the CFNIS premises and, in privacy, apply the software program to the applicant's copy of the hard drive.

Counsel:

Lieutenant-Commander D. Reeves, Canadian Military Prosecution Service, Counsel for Her Majesty the Queen

Lieutenant-Commander B.G. Walden, Directorate of Defence Counsel Services, Counsel for Corporal McGoey