COURT MARTIAL

Citation: *R v Holloway*, 2013 CM 1015

Date: 20131212
Docket: 201360

Standing Court Martial

Canadian Forces Base Edmonton
Edmonton, Alberta, Canada

Between:

Her Majesty, the Queen

- and –

Master Corporal C.J. Holloway, Accused

Before: Colonel M. Dutil, C.M.J.

RESTRICTION ON PUBLICATION

Restriction on publication: By court order made under section 179 of the *National Defence Act* and section 486.4 of the *Criminal Code*, information that could identify any person who is the subject of a representation, written material or a recording that constitutes child pornography within the meaning of section 163.1 of the *Criminal Code*, shall not be published in any document or broadcast or transmitted in any way.

REASONS FOR FINDING

(Orally)

[1] Master Corporal Holloway is charged with two offences; namely possession of child pornography, contrary to section 163.1 (4) of the *Criminal Code* and accessing child pornography, contrary to section 163.1 (4.1) of the *Criminal Code*. Both offences are punishable under section 130 of the *National Defence Act.* The alleged offences would have been committed at or near Camp Phoenix, Kabul, Islamic Republic of Afghanistan, on or about 19 June and 16 June 2011 respectively.

[2] The evidence consists of the following:

(a) the testimonies, in order of appearance before the court, of Mr T. Latta (formerly Master Corporal), Mr. M.J.S. Lalande (formerly Sergeant), Sergeant P.A. Hird, and Sergeant D.A. Corneau;

(b) Exhibit 3, which is a plastic bag containing a laptop computer, Alienware, an A/C cord, a Logitech webcam, and a Microsoft wireless receiver; all property of Master Corporal Holloway;

(c) Exhibit 4, a booklet containing seven photographs taken by Sergeant P.A. Hird on 20 June 2011 of and in the room shared by Master Corporal Latta and Master Corporal Holloway at Camp Phoenix during the alleged events;

(d) Exhibit 5, a booklet of four pictures of the computer screen of Master Corporal Holloway that were taken by Master Corporal Latta as it appeared then on 20 June 2011. These photographs are also found within the forensic report filed as Exhibit 6;

(e) Exhibit 6, a counsel mutually agreed version of a Canadian Forces National Investigation Service Computer Forensic Analysis Report, GO 2011-15506, made by Sergeant, then Master Corporal, Daniel Corneau, with regard to the alleges offences; more specifically with regard to the examination of the seized devices involved in this case, including the contents of the laptop computer listed at Exhibit 3;

(f) the matters for which the court has taken judicial notice under section 16 of the Military Rules of Evidence with regard to time zones between 16 June 2011 and 19 June 2011, namely that UTC (Coordinated Universal Time) equalled Eastern Daylight Time plus four hours and that AFT (Afghanistan Time) equalled UTC plus 4.5 hours; and

(g) the facts and matters for which the court has taken judicial notice under section 15 of the Military Rules of Evidence.

[3] The alleged events occurred at Camp Phoenix, Kabul, Islamic Republic of Afghanistan during OP ATTENTION, Roto 1, where Master Corporal Holloway was part of the advanced party as the chief signaller. They had arrived at Camp Phoenix in late April/May 2011. Master Corporal Holloway shared a room with Master Corporal Latta, who was a section commander within Niner Niner and also played a force protection role for the commanding officer and the regimental sergeant major. They shared room 17 in a building called "RLB 4." Prior to the deployment, they knew of each other, but were not personal friends. Exhibit 4 contains seven pictures of the room shared by the two individuals. Each occupant was issued one key to the room and it

was common practice that the room would be secured at all times when both occupants were not in the room.

[4] As they were on the advance party, no prior arrangements had been put in place to provide the members with computer equipment and facilities to communicate with their families as part of the troop's welfare programme. However, for those persons who had brought their own laptop computer, they could retain the services of the local Afghan Internet service provider, IO Global, and seek reimbursement. Master Corporal Holloway had brought his Alienware laptop computer, but Master Corporal Latta had not. In late May 2011, Holloway and Latta verbally agreed that they would share the Alienware laptop computer and that Master Corporal Holloway would seek reimbursement for the Internet connection. Master Corporal Holloway would pay for the first six months of the deployment and Master Corporal Latta would then pay and be reimbursed for the following six months. It appears that the Internet connection provided by IO Global was particularly slow. They had shared the computer for a period of three to four weeks prior to 19 June 2011.

[5] The shared laptop could be accessed in two ways: firstly, the user could type a common password which was "3PPCLI"; or secondly, the user could use a retina scan process. Master Corporal Latta only used the method with the password. Master Corporal Latta said that Master Corporal Holloway spent a lot of time on the computer and that he used it himself only to check emails and surf the net, mostly for reading newspapers or news platforms. However, Master Corporal Latta stated during cross-examination that he knew that his roommate's computer contained pornography, that he had looked at it before, only once he said, and that he knew where it could be found on the computer. Latta added that he did not have any folders stored or downloaded anything on the Alienware computer. Master Corporal Latta testified that Master Corporal Holloway spent a lot of time on his computer and that he had memory sticks and external hard drives.

[6] Master Corporal Latta testified that at approximately 2330 hours AFT on 19 June 2011 or within one hour each way, so plus or minus 2330 hours, he had returned to his room to check his emails and to look at the news on the computer. Master Corporal Holloway was on shift at the Tactical Operational Center, the TOC, until 2330 or 2400 hours that day. Master Corporal Latta stated that as he was logging off the computer, he clicked on the "Start Menu." As he was manipulating the computer mouse, the cursor had scrolled down to "Recent Downloads." He said that he then saw a filename that appeared to him to be downloading with a title saying something about a 13 year old girl. Master Corporal Latta testified that he then realized that there was something on the laptop that he did not want to be part of. Accordingly, he did not want to go any further and, according to his version of events, immediately went on the second floor to alert Sergeant Lalande about what had happened to him.

[7] Sergeant Lalande testified that Master Corporal Latta's voice was shaking and that he was visibly upset when he showed up at his room located on the second floor. Sergeant Lalande accompanied him to his room at Latta's request. Then they would

have opened two or three files folders on the C Drive in the folder "Media Files" to make sure that his concerns were legitimate and, according to Master Corporal Latta, the titles of the files and their contents matched. However, the witness said in cross-examination that he and Sergeant Lalande may have opened as much as 11 files during the evening of 19 June 2011. According to Latta's version of events, Sergeant Lalande opened these files, but they both looked at the images.

[8] Master Corporal Latta said that they then logged off from the computer and he reported his discovery to his chain of command at 0730 hours on 20 June 2011. Master Corporal Latta stated that after Sergeant Lalande went back to his room, he did not open any other file or folder to view images or videos. After speaking to Captain Jasper, the regimental sergeant major, Cavanaugh, and the commanding officer, Master Corporal Latta returned to his room. He then logged on the computer in order to take pictures of the computer screen, in particular of the "Download History" to show his chain of command. Master Corporal Latta stated that he never touched the computer after that moment.

[9] Master Corporal Latta said that both he and Sergeant Lalande were concerned about their discovery found on the accused's computer and that they should bring the matter forward to the chain of command. As I stated previously, Master Corporal Latta did not want to be associated with any impropriety. In contrast, Sergeant Lalande stated that he accompanied Master Corporal Latta to his room on two occasions during the evening of 19 June 2011. Sergeant Lalande's recollection of the events differs on several points. Sergeant Lalande stated that Latta's first visit to his room was at approximately 2100 hours as he was watching a movie. Master Corporal Latta told him that he had found files on the accused's computer that were indicative of child pornography. Sergeant Lalande asked Latta to show him. Back to his room with Sergeant Lalande, Master Corporal Latta used the computer mouse to move the arrow to "Recent Documents or Downloads." Sergeant Lalande then saw a list of files that appeared on the screen, where Master Corporal Latta took a step backwards as if he did not want to see anything on the screen. Sergeant Lalande told Latta that this could be a matter of perception and he then clicked on a file which indicated that the file did not exist. Lalande then told Latta that if he was still uncomfortable, Master Corporal Latta could report it to his chain of command. Sergeant Lalande would then have returned to his room. Master Corporal Latta would have returned to Sergeant Lalande's room again 10 minutes later to tell him then that he had found more files that raised concerns. Sergeant Lalande accompanied Master Corporal Latta again to his room. A video had started that showed a couple that appeared underage or young to him. In cross-examination, Sergeant Lalande said that the girl or lady appeared to be young, but that she did not have an ID card; meaning that he could not be certain of her age. The screen capture measured approximately four by four inches. Again, Sergeant Lalande told Latta that if it bothered him that much, he could contact his chain of command. Sergeant Lalande stated that he did not open any more files.

[10] Further to the allegations brought forward by Master Corporal Latta, a police investigation began on 20 June 2011. The investigation was led by Sergeant Hird, who

was at the time with the National Investigation Service Detachment located in Kandahar. Sergeant Hird arrived at Camp Phoenix, in Kabul, at approximately 1800 hours. During his investigation, he met with Master Corporal Latta at 2100 hours and Master Corporal Latta handed over his digital camera with which he had taken pictures of Master Corporal Holloway's Alienware computer screen earlier that day. Sergeant Hird recalled that he was surprised that Master Corporal Latta provided so much detail during the interview.

[11] Although Master Corporal Latta showed him the pictures he had taken through the digital display of the said camera, Sergeant Hird was unable to determine the age of the females who appeared on the pictures as they were too small; however, he believed the titles were consistent with child pornography. Sergeant Hird also interviewed Sergeant Lalande. Prior to leaving Camp Phoenix, Sergeant Hird had seized six items, namely: a laptop computer; a USB wireless device; a Logitech webcam; an external hard drive; an iPod, and a Microsoft X-Box console. In addition he had retained the Sony digital camera and a Sony 1GB memory stick that belonged to Master Corporal Latta.

[12] On 28 November 2011, Sergeant Corneau began the forensic analysis of the items seized during the investigation further to the allegations made by Master Corporal Latta. Sergeant Corneau testified during the trial to describe the results of his computer forensic analysis. The court was satisfied that Sergeant Corneau could testify as an expert witness to provide his observations and descriptions that were related to the conduct of his work as it relates to this particular case generally. However, the court was not satisfied that his limited credentials and experience were sufficient to enable him to offer expert opinion in such areas as categorization, the maturation stages of youth indicative of age in child pornography, and the preparation of computer analysis reports. The court allowed Sergeant Corneau to describe computer crime activities related to child pornography; to explain what are computer imaging and data storage systems; to explain the various methods, hardware and software used for the extraction of data from computer and data storage systems; to explain what peer-to-peer networks are and how they are used in child pornography related computer activities; and to describe and explain the language and terms used in computer activities related to child pornography, including filenames found in a computer or other electronic devices. He gave several examples of common terms normally associated with child pornography such as "Lolita," "PTHC," "PTSC," "Hussyfan," "8yo," etc. Sergeant Corneau described the results of his forensic examination of the items found in Master Corporal Holloway's laptop internal hard drive including the files found, their location, and details about them, i.e., when were they created, downloaded, accessed, and transferred.

[13] Sergeant Corneau testified that he started his analysis of Master Corporal Holloway's laptop hard drive on 28 November 2011 using the Tableau Forensic Imaging Software Version 1.11 and the Tableau eSATA Bridge Write Blocker. Once he had acquired the contents of the computer internal hard drive, Sergeant Corneau scanned the said hard drive for viruses, and no threats were identified. The computer hard drive was partitioned into:

(a) C: the operating system partition; and

(b) D: file recovery partition.

Sergeant Corneau used two special softwares or programmes to conduct his forensic analysis, namely EnCase and C4All (C4All stands for Categorizer for Pictures and Videos). These softwares serve to acquire and analyse the data, extract the pictures and videos found in the hard drive, as well as all the technical information associated with these images and videos. For example, the EnCase will perform a hashing of the device being analysed. This programme would give the operator the name of the file, its location or locations on the hard drive, when the file was created, and when it was last accessed.

[14] Sergeant Corneau testified that he found 129,771 images and 14 videos on the internal hard drive. Of those images, 97 were consistent with child pornography, but only 40 of them were accessible to a user according to the software C4All. Sergeant Corneau stated that he sent 39 of the images to the RCMP to verify the MD5 hashes; 57 images were found in unallocated clusters or recovered folders.

[15] Sergeant Corneau testified that although file names can match the content of an image or video file, it is not always true. His testimony also revealed that whenever the programme C4All provides information such as when a file was created and last accessed, this term does not mean that the user opened a file. During his testimony, Sergeant Corneau explained at length how the "Recent Items List" seen on a computer screen was structured. He stated that the first files displayed were those that began with special characters, then by those files beginning with numbers, and finally the files with letters. Each of these three categories listed files similar in nature in chronological order after. He stated that the screen showing a "Recent Items List" would only display the 15 most recent items, where the computer registry keys would provide more information and organize it in a different way. I refer to pages 232 to 241 of Exhibit 6.

[16] Sergeant Corneau testified extensively with regard to specific images and videos that he found during his analysis. I will refer to some elements of his report further in this decision. He explained that a significant number of the material found in the computer had identical creation and access dates because they had been obtained from another media or external device during what he believed to be a mass transfer as opposed to a download from the Internet. Also, the specific times attached to these creation and access dates were identical or closely related.

[17] The forensic report that Sergeant Corneau filed, at Exhibit 6, indicates that a significant amount of images were found in several locations or clusters on the laptop's internal hard drive, but his report does not provide information that would give elements as to when a user modified a file. He stated, however, that the access date of a file containing an image or video can be set in four ways:

(a) when a user opens the file;

(b) when a user modifies a file;

(c) when the computer displays a file in thumbnail view; or

(d) when an automated process scans folders and files, such as antivirus software.

[18] Sergeant Corneau readily agreed than the access date of a file is not necessarily changed only when a user opens that file. He said that a specific analysis is required to find why a specific access date was changed. Sergeant Corneau testified that he did not perform that analysis in this case to determine if the computer was modified by the user to deal with access dates or to determine what software programmes may have been on the computer to view images or video files that were able to change the access dates for those files.

[19] Sergeant Corneau also testified that when a file has identical creation and access dates, it is most likely that such file was not opened by the user unless the access date was previously set by the user in a manner previously described.

[20] Sergeant Corneau testified that some pictures had distinctive elements or watermarks that were commonly seen in child pornography images, such as "LS Models," although he could not explain how and when those watermarks ended up on the images, nor that a user typing this term would reveal a specific image while surfing on the Internet.

[21] Sergeant Corneau testified that he did not recall, nor was he asked to verify whether the computer analysed contained any peer-to-peer software or that such networks were ever used on that computer. He stated that he found no evidence that the accused or a user of that computer named a specific suspect file on this computer. Sergeant Corneau believed that all the files transferred on the computer on 16 June 2011 came from another device, not from the Internet. These files were described in the following way: 39 accessible images files and 12 accessible video files.

[22] Importantly, Sergeant Corneau said that he did not conduct or was asked to do any analysis of the following matters, as he could have done so:

(a) when the folders and files were created;

(b) when the folders and files were transferred on 16 June 2011, how many folders or files were transferred; and

(c) if any user other than Master Corporal Holloway could have transferred files or renamed a folder from the device. Sergeant Corneau was very candid during his testimony with regard to his minimal level of

> experience at the time he performed the analysis of Master Corporal Holloway's computer. He testified that his reports are now more in-depth and that the type of information that I have just described would now be included in these reports.

[23] Sergeant Corneau also stated that the only other device analysed was the 1 Terabyte Western Digital External Hard Drive that was seized at the time. No material that could constitute child pornography was found in this device. The device from which the data was transferred on 16 June 2011 was not found.

[24] Subsections 163.1(1), (4), (4.1) and (4.2) of the *Criminal Code* read as follows:

> (1) In this section, "child pornography" means
>
> (*a*) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,
>
> (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or
>
> (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;
>
> (*b*) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act;
>
> (*c*) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or
>
> (*d*) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act.

Subsection (4) says:

> (4) Every person who possesses any child pornography is guilty of
>
> (*a*) an indictable offence and is liable to imprisonment for a term not [exceeding] five years and to a minimum punishment of imprisonment for a term of six months; or
>
> *(b)* an offence punishable on summary conviction and is liable to imprisonment for a term not [exceeding] than 18 months and to a minimum punishment of imprisonment for a term of 90 days.

Subsection (4.1) reads:

> (4.1) Every person who accesses any child pornography is guilty of
>
> (*a*) an indictable offence and is liable to imprisonment for a term of not more than five years and to a minimum punishment of imprisonment for a term of six months; or
>
> (*b*) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.

Subsection (4.2) reads:

> (4.2) For the purposes of subsection (4.1), a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself.

[25] The court cannot find Master Corporal Holloway guilty of the first charge, namely possession of child pornography, unless the prosecution has proved beyond a reasonable doubt that he is the person who committed the offence on the date and in the place described in that charge; that is, on or about 19 June 2011, at or near Camp Phoenix, Kabul, Republic of Afghanistan. Specifically, the prosecution must prove each of the following essential elements of the offence beyond a reasonable doubt: the existence of a photographic, film, video or other visual representation constituting child pornography; and that the accused was in possession of a photographic, film, video or other visual representation constituting child pornography.

[26] With regard to the second charge, namely accessing child pornography, unless the prosecution has proved beyond a reasonable doubt that he is the person who committed the offence on the date and place described in that charge; that is, on or about 16 June 2011, at or near Camp Phoenix, Kabul, Republic of Afghanistan. Specifically, the prosecution must prove each of the following essential elements of the offence beyond a reasonable doubt: the existence of a photographic, film, video or other visual representation constituting child pornography; that the accused caused child pornography to be viewed by, or transmitted to, himself or herself; and that the accused knew that he caused child pornography to be viewed by, or transmitted to, himself or herself.

[27] In *R v Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, Justice Fish, for the majority, expressly stated the prerequisite for an offence of possession of child pornography and the distinct offence of accessing child pornography, at paragraphs 14 to 16:

> [14] In my view, merely viewing in a Web browser an image stored in a remote location on the Internet does not establish the level of control necessary to find possession. Possession of illegal images requires *possession of the underlying data files in some way*. Simply viewing images online constitutes the separate crime of *accessing* child pornography, created by Parliament in s. 163.1(4.1) of the *Criminal Code*.

> [15] For the purposes of the *Criminal Code*, "possession" is defined in s. 4(3) to include *personal possession*, *constructive possession*, and *joint possession*. Of these three forms of culpable possession, only the first two are relevant here. It is undisputed that *knowledge* and *control* are essential elements common to both.
>
> [16] On an allegation of *personal possession*, the requirement of knowledge comprises two elements: the accused must be aware that he or she has physical custody of the thing in question, and must be aware as well of what that thing is. Both elements must co-exist with an act of control (outside of public duty): *Beaver v. The Queen*, [1957] S.C.R.531, at pp. 541-42. [emphasis in original]

And then Fish, C.J. set in its proper context how this offence has a particular dimension when images and videos are stored as digital files, and we can find that at paragraphs 18 and 19 of the decision:

> [18] Here, the appellant is alleged to have had possession of digital images in a computer, rather than tangible objects. The law of possession, however, developed in relation to physical, concrete objects. Its extension to virtual objects — in this case, images stored as digital files and displayed on computer monitors — presents conceptual problems. Unlike traditional photographs, the digital information encoding the image — the image file — can be possessed even if no representation of the image is visible. Likewise, even if displayed on a person's computer monitor, the underlying information might remain firmly outside that person's possession, located on a server thousands of kilometres away, over which that person has no control.
>
> [19] Essentially, there are thus two potential "objects" of possession of an image in a computer
> — the image file and its decoded visual representation on-screen. The question is whether one can ever be said to be in culpable possession of the visual depiction alone, or whether one can only culpably possess the underlying file. Canadian cases appear implicitly to accept only the latter proposition: That possession of an image in a computer means *possession of the underlying data file*, not its mere visual depiction. [emphasis in the original]

[28] The first and most important principle of law applicable to every criminal case or offences dealt with under the Code of Service Discipline is the presumption of innocence. Master Corporal Holloway entered the proceedings presumed to be innocent, and the presumption of innocence remains throughout the case unless the prosecution, on the totality of evidence, satisfies the court beyond a reasonable doubt that he is guilty. The burden of proof rests with the prosecution and never shifts. There is no burden on Master Corporal Holloway to prove that he is innocent. He does not have to prove anything.

[29] A reasonable doubt, as we know, is not an imaginary or frivolous doubt. It is not based on sympathy or prejudice against anyone involved in the proceedings. Rather it is based on reason and common sense. It is a doubt that arises logically from the evidence or from an absence of evidence. It is virtually impossible to prove anything to an absolute certainty, and the court is not requiring the prosecution to obtain that level of certainty. Such a standard is impossibly high and is not in accordance with our law.

However, the standard of proof beyond a reasonable doubt falls much closer to absolute certainty than to probable guilt.

[30] There is no issue in this case that the laptop computer where the material was found is the property of Master Corporal Holloway and that he was the main user of that computer. However, he had been sharing his computer with Master Corporal Latta for a period of three to four weeks when the alleged offences would have occurred. There is also no issue that some of the material found on the computer would constitute child pornography under section 163.1 of the *Criminal Code*. However, the evidence relied on by the prosecution to establish the elements of possession and accessing child pornography is significantly circumstantial. The court must be satisfied beyond a reasonable doubt that the Master Corporal Holloway's guilt is the only rational conclusion to be drawn from the whole of the evidence or from an absence of evidence.

[31] It is not unusual that some evidence presented before the court may be contradictory. Often, witnesses may have different recollections of events. The court has to determine what evidence it finds credible. As we know, credibility is not synonymous with telling the truth, and a lack of credibility is not synonymous with lying. The court is not required to accept the testimony of any witness except to the extent that it has impressed the court as credible. However, a court will accept evidence as trustworthy unless there is a reason to disbelieve that evidence.

[32] The court finds that the testimony of Master Corporal Latta is problematic in many ways. There is no doubt that he was seriously concerned when he saw some of the material found on Master Corporal Holloway's computer during the evening of 19 June 2011, namely the file names that he described and the images in thumbnail view. He was so concerned that he alerted Sergeant Lalande and even took pictures of the computer screen the next day. However, he could not convince Sergeant Lalande of the seriousness of his allegations after two attempts to show him some files on the computer. Sergeant Lalande basically told him that if he felt so concerned about what he had found, that Latta should report it to the chain of command. However, the court is convinced that those pictures reproduced at Exhibit 5 and contained in the report filed at Exhibit 6 are not indicative of what Mr Latta said originally to have seen. They are not the same that were on the screen content when we look at what would have been there on 19 June 2011 when he looked at the computer screen and when he took those photographs on 20 June 2012; that is, the next day.

[33] The court reached this conclusion in assessing the entire testimony of Mr Latta with the testimony and the opinion of Sergeant Corneau with regard to his analysis of the computer and the information revealed by the registry keys of the computer found at pages 232 to 240 of Exhibit 6. The court also does not accept the theory of the prosecution that Master Corporal Latta was not computer savvy to the extent that he could only use a computer to view emails and access Internet sites to watch the news. Sergeant Lalande may have witnessed before that Mr Latta appeared to need some help to attach photos to emails sent on the DWAN or that Master Corporal Latta had sent an email to the RSM by mistake, the rest of the evidence clearly demonstrates that he could

not only navigate on the Internet to watch the news and manage his email account, but that he was also capable of accessing files on a computer, including the accused's computer that he had been sharing with him between three to four weeks. For example, he knew how and where to access pornography on that computer and he had done so at least on one occasion. His version of events is not supported by the analysis of Sergeant Corneau as to the number of files that he had opened or said that he had opened or accessed on 19 June 2011 between 2130 hours and 2400 hours with or without Sergeant Lalande.

[34] The court does not believe that witness when he said that he was simply consulting the news or looking at his emails when the cursor would have moved accidently to the recent items list. His testimony is almost *chirurgical* for events that occurred more than two years ago. The court believes the witness when he says that he was terribly concerned about some elements that appeared to him on 19 June 2011, and he did not want to be implicated or associated with the perceived or real presence of child pornography on the shared computer. However, I have serious doubts that the manner in which he found the troubling material is as accidental as what he has described before the court. The report and the testimony of Sergeant Corneau about the information contained in the computer registry keys clearly demonstrates that someone accessed several litigious computer files during the critical period, where Master Corporal Holloway was not even present in his room.

[35] The prosecution alleged that all of the 97 image files and the 14 video files found on Master Corporal Holloway's computer constitute child pornography. Several images are from pre-pubescent children and fall squarely within the definition of child pornography. These images are found at Exhibit 6, pages 35, 48, 49, 60, 63, 72, 77, 82, 93, 110, 115, 123, 173, 187, and 190. The prosecution also submitted that the other images depicted at Exhibit 6 show young persons in various stages of puberty that the court should accept as child pornography in considering various factors or indicia such as breast and labia development; absence of pubic hair; the skin; any marks that are indicative of a person that is older such as marks, blemishes, wrinkles, etc. or any other marks that would normally be found on a child or would not be found on a child. The prosecution asked the court to also focus on the settings surrounding these images in making its assessment.

[36] The prosecution submitted that the evidence clearly indicates that Master Corporal Holloway had the necessary knowledge and control of the material that he clearly personally possessed on his computer. They do not rely on constructive possession or joint possession.

[37] The prosecution argued that the evidence establishes that the massive transfer of data from an external device that occurred on 16 June 2011 could only be done by Master Corporal Holloway and not by anyone else, including Master Corporal Latta. The prosecution also submitted that the amount of data transferred was so extensive that Master Corporal Holloway ought to be aware of it. In addition, the prosecution refers to the Summary Report at pages 242 and 246 of Exhibit 6 to show that the material

transferred on the computer on 16 June 2011 came from an external media storage device from an assigned "G Drive" and asked the court to infer that this device belonged to Master Corporal Holloway, and that he knew of its content on the basis of Master Corporal Latta's testimony that Master Corporal Holloway possessed such device on a shelf in the room.

[38] There is no evidence that a specific USB Media Storage Device was used to transfer the data on the computer on 16 June 2011. We know that one was used, but a specific USB Media Storage Device we do not. No such device or devices were ever found in the room, but that is not to say that it never existed, but there's an absence of evidence about that device being found in the room. Although the court may infer that the device used on 16 June 2011 used to transfer a massive amount of files that contained pornographic material on the computer, including child pornography, did not belong to Mr Latta and likely to Master Corporal Holloway, this evidence alone is not sufficient to conclude that Master Corporal Holloway knowingly caused child pornography to be viewed by or transmitted to himself.

[39] The prosecution also stated that the accused could not say he did not know the presence of the material found on his computer because of the large transfer of data that occurred on 16 June 2011. They advanced four reasons in support of their position:

(a) the evidence shows that it is Master Corporal Holloway that transferred the material;

(b) the videos and names that were transferred are indicative of child pornography and that the media player indicates that on 16 June 2011, there were videos watched that had names indicative of child pornography;

(c) some of the files transferred on 16 June 2011 were later deleted by the user, which they suggest can only be by Master Corporal Holloway; and

(d) that there were duplicate child pornography files on the computer dating back from 2007 and 2008.

[40] The prosecution asked the court to review Exhibit 6 at page 24, location 4, and see that the file path shows the name of the accused himself as well as many others images including those at page 82, location 33; 119, location 18; 128, location 4; 160, location 22; and 201, location 1. They submit that all these files were deleted by the accused because his name appears in the file extensions and also his name is in the file architecture that was transferred over. Because deleted files or deleted folders are not transferred from an external device, the prosecution suggested that the accused had to go into a folder where a file was located, click on that file and delete the data. The prosecution asked the court to draw the following inferences:

(a) that the accused knew how to get to the file and knew that a file existed;

(b) that he knew the nature of those files, at least by their names;

(c) some of the files had previously been on his computer, for example, on 4 June 2011 and 16 June 2011, 16 June 2011 and 22 November 2008, deleted afterwards, and 16 June 2011 and 6 May 2009, deleted afterwards. In addition, the prosecution points to those three videos where the dates are before the accused's deployment to Kabul in 2011.

[41] As to the element of control, the prosecution relied on following elements:

(a) the fact that the accused owned the computer;

(b) the testimony of Master Corporal Latta who said that the accused spent a lot of time on his computer;

(c) the fact that Master Corporal Holloway had set a password and retina scan to access the computer; and

(4) the accused's laptop was kept in a room shared only with his roommate, Latta, and the door was locked at all times to prevent access.

[42] For the prosecution it is clear that Master Corporal Holloway has accessed child pornography on 16 June 2011. They rely on the following elements, namely: the facts that the accused owned the password protected computer; only the accused and Latta had access to the computer; Latta did not store any item on the computer and was an unsophisticated user; Latta did not think of bringing his own computer to Kabul initially; and that the defence never put to Mr Latta in cross-examination that it was him that transferred the data on the computer.

[43] Counsel for the defence was strongly opposed to the inferences sought by the prosecution. No evidence was presented on behalf of Master Corporal Holloway as they did not have to; it is for the prosecution to prove its case beyond a reasonable doubt. Therefore, the court will determine first whether there is evidence beyond a reasonable doubt that the accused accessed any alleged image or video files on 16 June 2011, and, second, whether the accused was in possession of any alleged image or video files on 19 June 2011. If so required, I will then determine if any of these image or video files constitutes child pornography.

[44] Although it is reasonable to draw an inference that the sole owner of a password protected computer is, in absence of evidence to the contrary, the person that can access that computer, this statement does not hold up to scrutiny where the evidence indicates that such computer is shared by more than one person, regardless whether this situation has existed for four weeks or four years.

[45] The evidence of Sergeant Corneau indicates that whether a file has a creation date and an access date does not necessarily mean by itself that a user has viewed an image or video file or has knowingly caused these images or video files to be viewed by, or transmitted to, himself or herself. Similarly, the fact that image or video files are found on a computer hard drive, does not allow someone to draw an inference that the user knew of their existence and exercised control over them. In a decision of the Ontario Court of Justice that strikingly resembles in many aspects to this case, MacDonnell, J. stated in *R v Garbett*, 2008 ONCJ 97, 4 March 2008, at paragraph 24:

> Accordingly, the mere fact that an image was found on a computer's hard drive does not lead inexorably to an inference that the user knew of its existence, or that the user had ever viewed it, intended to view it, intended to save it, or did anything to cause it to be saved. Constable Lancaster's evidence makes clear that to support any of those inferences, there must be something more.

[46] The testimony of Sergeant Corneau is also abundantly clear on this point. Moreover, he confessed that his analysis could have been more comprehensive. I believe a more in-depth analysis of the computer would have likely helped to support the theory of the prosecution or at least provide stronger circumstantial evidence capable of supporting the inferences sought by the prosecution. With regard to all image files that were either referred to as deleted files, recovered folders or found in unallocated clusters, Sergeant Corneau testified that these files are not accessible to an average user, unless that user has special knowledge and the necessary software to make them accessible. There is no evidence to support this possibility. In such circumstances, in absence of more analysis, it is not possible to determine whether these files were created, accessed or viewed by a user or deleted.

[47] The court is not in a position to speculate with regard to any of those files that were recovered by Sergeant Corneau during his forensic computer analysis. There is simply no reasonable means for the court to infer possession or access by the accused of those inaccessible files. The evidence before the court indicates that 57 image files out of 97 image files and four video files were inaccessible on the computer because they were in recovered folders or unallocated clusters. The image file located at page 97 of Exhibit 6 was accessible and it indicates a creation and access date of 8 May 2008, within a window of approximately 90 minutes. As mentioned by the prosecution, the four video files found at pages 192, 200, 202, and 203, all at location 1, have a creation date of 4 June 2011.

[48] The large amount of data transferred on 16 June 2011 from an external device included 39 accessible image files and 12 accessible video files. It is the computer who attributed these files with that creation date. The defence submitted that the evidence likely supports the proposition that prior to 16 June 2011, 57 image files and one video file of alleged child pornography had been deleted from the accused's laptop computer. I accept that this statement is supported by the report at Exhibit 6 and also by the testimony of Sergeant Corneau. The evidence indicates also that on the evening of 19 June 2011, Mr Latta and probably Mr Lalande opened files on the accused's computer, and that Mr Latta did so again the following morning.

[49] The second charge alleges that Master Corporal Holloway accessed child pornography on 16 June 2011. The prosecution alleges that he would have done so three days prior to Mr Latta's actions on that laptop computer. The access would correspond to the transfer of data between the unknown device and the laptop computer. I accept the theory of the defence that this charge relates to 39 images and 12 videos that were accessible by a user. Accepting the proposition that the transfer of data was not done by Mr Latta, it is reasonable that this transfer is more than likely the result of Master Corporal Holloway's own input. However, there is insufficient compelling evidence to show that the accused knew of the mere existence of child pornography in the large number of files that were transmitted, albeit the court concludes on the totality of the evidence that Master Corporal Holloway knew that it contained pornography.

[50] There is no evidence before the court that the accused created any of these files transferred on the 16th of June, 2011 or that he opened any of these folders, subfolders or sub-subfolders. There is no evidence that Master Corporal Latta owned the device used to transfer the data or any evidence that he knew of its content and the likelihood that it could contain child pornography. Therefore, if the court may conclude that Master Corporal Holloway caused child pornography to be viewed by, or transmitted to him, the prosecution has failed to demonstrate the element of the offence that requires that the accused did access the said material knowingly, in absence of additional evidence.

[51] As to the first charge; that is, the possession of child pornography on or about 19 June 2011, the court accepts that Sergeant Corneau determined that 57 image files and four video files were found on the computer through special equipment normally not available to an average user. These files were found in unallocated clusters or were designated as recovered folders. They were not accessible to the computer user. The analysis did not indicate if any of those files were transferred from another device and they had been deleted prior the seizure of the computer by Sergeant Hird. We know that the possession of an image in a computer means possession of the underlying data file, as long as the person who is alleged to possess that file has knowledge and control of that data file.

[52] The defence argued that there is no evidence that the accused intended to possess these files because they were deleted, and he could not exercise control over them as they had become inaccessible. This submission has merit when we examine the situation as it existed on or about 19 June 2011, but it may not have merit if one would look at an undefined earlier period where those files would have been accessible. However, it is not for the court to speculate on this matter or make inferences in absence of additional evidence.

[53] Accepting that the computer hard drive had approximately 40 image files and 14 or 16 video files that were accessible to a user when it was seized, the defence suggested that there is little evidence as to who would have installed those files on the accused's computer. I accept that the court may infer that it was done by Master

Corporal Holloway based on the evidence, however, it cannot be inferred without any additional evidence that the accused knew of the nature and the content of these files or that he opened these files or ever viewed them prior to 19 June 2011. We know that there was a massive transfer of data files on 16 June 2011, more than likely by Master Corporal Holloway.

[54] The prosecution relied on the report at Exhibit 6 to submit that the video files with a creation date of 4 June 2011 ought to be possessed by the accused because they were already on the computer prior to the massive transfer. Again, there is no evidence if those files were ever opened or viewed by the accused or that he was aware of their existence and content in the context of the presence of over 100,000 images and videos found on the computer. It is unknown also when those videos were transferred.

[55] Sergeant Corneau has found that 39 images located in the folder Files\Microsoft Favorites\Young\Pictures had identical creation and access dates. However, the analysis did not establish whether any of those images were ever viewed. As to the image with a creation date of 8 May 2011, at page 97 of Exhibit 6, there is no evidence before the court that would indicate how this image found its way on the hard drive to assist the court to attribute knowledge and control to the accused in the context that that image was amongst more than 100,000 other images. The court understands that this information could have been obtained, at least in part, if the expert had conducted a more in-depth analysis of the laptop internal hard drive.

[56] There is also no evidence that would support any inference that Master Corporal Holloway structured or named folders or subfolders on his computer in a meaningful way or in attempt to deceive or hide the content of files in placing them in sub-subfolders. For example, files were contained in Program Files\Microsoft Favorites\Young\Pictures\28 Paczka, and then you have Files\Microsoft Favorites\Young\Pictures\30 Paczka, Files\Microsoft Favorites\Young\Pictures\Amatour4chantop, Files\Microsoft Favorites\Young\Pictures\4Chantop, this time with a capital C.

[57] A thorough review of the architecture of the folders and files cannot support the view that Master Corporal Holloway had put in place a system of organization to manage these files or that would at least support an inference that he knew of their nature or their content. For those files that show Master Corporal Holloway's name in the file path, they were all recovered and inaccessible files. There is no evidence to support that the accused ever opened or viewed these documents. In any event, they were not under his control on the alleged date. Whether they may have been under his control three years ago is a whole different story, but there again, there is no evidence for the court to draw that inference.

[58] As to the evidence of file names indicative of child pornography such as "Lolita," "PTHC," "PTSC," "Hussyfan," "8yo," etc. found in the "Recent Items List" photographed by Mr Latta on 20 June 2011, the court can not infer that Master Corporal Holloway knew of it in light of the testimonies of Mr Latta and Sergeant Corneau that

tend to establish that these files had been recently opened by someone other than the accused on or about 19 June 2011. Unlike the presence of similar terms under the heading "Favorites" of the Internet browser computer user that would support a reasonable inference that the user browsed a web site that contained explicit images of females under the age of 18, it is not reasonable to infer from the mere presence of the file names on the recent items list of Master Corporal Holloway's computer that he shared with Mr Latta at the time, in the absence of evidence to the contrary or in absence of additional evidence, that he was aware of their nature or content, unless there was at least evidence that he had consulted that list or opened these files himself during the period that can be attached to that list. There again, the evidence to that fact is unsatisfactory.

[59] The prosecution has asked the court to draw several inferences against the accused in support of their position. Many of them are compelling, but many of them are not compelling because they are not only insufficiently supported by the technical evidence, but also because some additional evidence was available by the expert. Should the forensic computer expert have conducted a more in-depth review from the evidence seized at the time, as he readily admitted himself, the inferences sought by the prosecution would have potentially been exponentially stronger.

[60] The court is left with the belief that the prosecution may not have been fully aware of the shortcomings of the expert analysis and that Sergeant Corneau could have supplemented his report with relevant additional information before that was revealed during the very extensive cross-examination conducted by counsel for the defence. In light of the totality of the evidence, the court is convinced that Master Corporal Holloway is more than likely guilty of both offences as charged, but not beyond a reasonable doubt. Consequently that doubt must benefit the accused.

FOR THESE REASONS, THE COURT:

[61] **FINDS** Master Corporal Holloway not guilty of both charges.

Counsel:

Lieutenant-Commander S. Torani and Lieutenant-Commander D.T. Reeves, Canadian Military Prosecution Services
Counsel for Her Majesty the Queen

Lieutenant-Commander B.D. Walden, Directorate of Defence Counsel Services
Counsel for Master Corporal C.J. Holloway