COURT MARTIAL

Citation: *R. v. Machtmes*, 2021 CM 2006

Date: 20210517
Docket: 202035

General Court Martial

Bay Street Armoury
Victoria, British Columbia, Canada

Between:

Her Majesty the Queen, Applicant

- and -

Master Sailor R.D. Machtmes, Respondent

Motion heard and decision rendered in Victoria, British Columbia, on 16 March 2021.
Reasons delivered in Gatineau, Quebec, on 17 May 2021.

Before: Commander S.M. Sukstorf, M.J.

Pursuant to section 179 of the *National Defence Act* and section 486.4 of the *Criminal Code*, the Court orders that any information that could disclose the identity of the person described during these proceedings as the complainant, including the names of family members, addresses and any professional or nicknames used, or a witness, shall not be published in any document or broadcast or transmitted in any way, except when disclosure of such information is necessary in the course of the administration of justice, when it is not the purpose of that disclosure to make the information known in the community.

DECISION CONCERNING A *VOIR DIRE* TO DETERMINE ADMISSIBILITY OF INSTAGRAM MESSAGES

Introduction

[1] Master Sailor Machtmes is facing three charges. The first two charges are contrary to section 130 of the *National Defence Act* (*NDA*), that is to say, for luring a child and invitation to sexual touching, contrary to section 152 and paragraph 172.1(1)(b) of the *Criminal Code*. The

third charge relates to an allegation of disgraceful conduct contrary to section 93 of the *NDA*. The three charges before the Court emanate from the accused's alleged use of sexualized conversations via Instagram with a person presenting as a minor.

[2] At the opening of the General Court Martial, at the prosecution's request, the Court held a *voir dire* on the admissibility of a document containing ninety-eight screenshots depicting what purports to be direct messages exchanged between the Instagram account of "@randymanmax" and the Instagram account of a minor, C.L, who at the time was under the age of sixteen.

[3] The prosecution called three witnesses from Australia, which included C.L., who was the author of one side of the Instagram messages; his mother F.L., who discovered the messages; and the Parramatta, New South Wales, police officer, Constable Byrne, who took the photos of the Instagram messages and uploaded them into their police evidence management system. The defence entered no evidence on the *voir dire*.

[4] On consent, the prosecution admitted fourteen different exhibits which included an Agreed Statement of Facts. In their final representations, counsel advised the Court that they had narrowed the sole issue of admissibility down to whether or not the Instagram exchanges meet the requirements set out at sections 31.1 to 31.8 of the *Canada Evidence Act* (*CEA*). I considered their final submissions and analyzed the evidence against the law. After deliberating on the issue, the Court rendered a short oral decision on 16 March 2021, admitting the Instagram communications and indicated that detailed reasons would follow. These are the Court's written reasons on its decision made on the *voir dire*.

Position of the parties

Prosecution

[5] In their submissions, the prosecution made the following arguments:

(a) photographs of the Instagram communications are considered electronic documents under section 31.8 of the *CEA*;

(b) they have satisfied the admissibility requirements under the *CEA*; and

(c) no evidence of authorship is required.

Defence

[6] In his oral submissions, the counsel for the accused submitted the following arguments:

(a) Relying upon paragraph 7 of *R. v. Donaldson*, 2016 CarswellOnt 21760, [2016] O.J. No. 7153, 140 W.C.B. (2d) 513, defence argued that the photographs of the Instagram communications are not electronic documents under the *CEA* and are merely the equivalent of a cut-and-paste document as the court found in *Donaldson*; and

(b) Evidence of tampering. In responding to the prosecution's suggestion that there were no challenges to the authenticity of the documents due to tampering, he argues that the prosecution's own evidence suggests otherwise. He submitted that C.L. testified that the only communications he exchanged with "@randymanmax" were through Instagram. Given this, defence argues that there are inconsistencies that raise some concern. He further argues that since the police directed F.L. to delete the Instagram account C.L. was using, there is an inadequate record left to verify the conversations and therefore the burden on the prosecution has not been met.

Witness Testimony

[7] C.L. testified to having both an IPhone and an IPad, both of which he used to access his Instagram account. He testified that he used Wi-Fi to access Instagram on his IPad and data for his phone. He confirmed that his mother, F.L. had access to his devices. C.L. testified that the first time he received a private direct message from "@randymanmax" was on the occasion of his fifteenth birthday when he received a birthday greeting from him. C.L. acknowledged that after his mother discovered what she felt were inappropriate messages from "@randymanmax" she sent a few messages to the "@randymanmax" Instagram account using C.L.'s Instagram account. After the prosecution scrolled through all the Instagram messages with C.L., he confirmed for the court that they were the messages sent by "@randymanmax" and received by him.

[8] F.L. testified that she noticed C.L.'s Instagram messages on C.L.'s IPad while C.L. was at school. She explained that C.L.'s IPad was plugged into the family charging station and when C.L. received messages on his phone, they would also ping to C.L.'s IPad, so she looked at them. She testified that the messages were not appropriate for an adult-child discussion and she was not happy with the content of the conversations. She told the Court that she monitored the messages and messaged "@randymanmax" directly to try and scare him off, but when she was not successful, she took the IPad down to the Parramatta, New South Wales, Australia police station to seek their feedback. She was not sure if she was just being paranoid or whether she should be concerned. When asked whether the IPad from which she accessed the Instagram messages and later brought to the police station was functioning, she said it was functioning perfectly as the IPad was brand new.

[9] Constable Byrne from the New South Wales, Parramatta, Australian police testified that on 14 November 2018, F.L. brought C.L.'s IPad into the Parramatta police station seeking assistance. He told the Court that F.L. handed him the IPad and he opened the Instagram application which was already logged in to C.L.'s Instagram account because the password was saved on the IPad. After F.L directed him to the conversation, he reviewed the entirety of the messages. He testified that after consulting with his supervisor, he used his IPhone 7 Plus to take photos of the Instagram communications that took place between "@randymanmax" and C.L.'s Instagram account.

[10] He further testified that he created a case event and uploaded the photos directly into the police evidence management system, which is a secure platform. In doing so, he converted all the photos into one PDF file which was then preserved and linked to an investigative file number. He told the Court that once the file was uploaded to that system, it was secure and could not be changed. He testified that his IPhone 7 was working perfectly as was the IPad where he viewed the messages and he took the photos. He also testified that the police computer and system where he uploaded the photos were also functioning perfectly.

[11] With respect to the PDF file that was uploaded into the police evidence management system, he told the Court that he accessed the file a few times and that from his observations, the form and file were exactly the same. He told the Court he took ninety-nine photos, but realized that one of the photos was not relevant so there were a total of ninety-eight photos that relate to the matter before the Court. In direct examination by the prosecution, Constable Byrne reviewed the ninety-eight photos and confirmed for the Court that they were all the photos he took.

[12] Constable Byrne also told the Court that he advised F.L. to block the user account of "@randymanmax" or delete C.L.'s Instagram to ensure that "@randymanmax" could not contact C.L.

Issue

[13] The issue to be decided is whether or not the Instagram direct messages communicated between the "@randymanmax" Instagram account and the Instagram account of C.L. should be entered in as evidence.

The law

[14] In deciding on evidentiary issues related to the admissibility of evidence, a court martial must first look to the *Military Rules of Evidence* (*MRE*) for guidance. With respect to the admission of this type of record, the *MRE* are silent on how they should be introduced. However, in the event that the *MRE* do not provide for an evidentiary rule to deal with a matter, section 4 provides guidance.

[15] Section 4 of the *MRE* reads:

> **Cases Not Provided For**
>
> 4 Where, in any trial, a question respecting the law of evidence arises that is not provided for in these Rules, that question shall be determined by the law of evidence, in so far as it is not inconsistent with these Rules, that would apply in respect of the same question before a civil court sitting in Ottawa.

[16] Consistent with section 4 of the *MRE*, and as articulated at paragraph 3 of a decision of Paciocco, J (as he then was) of the Ontario Court of Justice in *Donaldson*, "The presentation of electronic evidence, whether it be Facebook messages, emails or text messages, or any other form of electronic communication, is governed by technical rules provided for in the *Canada Evidence Act* [(*CEA*)]." (see also *R. v. S.H.* 2019 ONCA 669 as affirmed by the Supreme Court of Canada (SCC) in *R. v. S.H.* 2020 SCC 3).

[17] Under the *CEA*, an electronic document is defined at section 31.8 as follows:

> ***electronic document*** means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data. (*document électronique*) [Emphasis added]

[18] Smart phones and other computing devices fall within the definition of "computer system" for the purposes of section 31.8 of the *CEA*. As such, the admissibility of Instagram messages and other electronic communications recorded or stored in a smart phone, IPad or other are governed by the *CEA* statutory framework (see *R. v. Ball*, 2019 BCCA 32 at paragraph 67).

[19] In short, there is a two-step process that must be followed for parties seeking the admissibility of electronic documents under the *CEA*.

(a) Step 1 – the person seeking to admit the electronic document has the burden of proving authenticity, pursuant to section 31.1 of the *CEA*; and

(b) Step 2 – the document must comply with the best evidence rule, pursuant to sections 31.2 and 31.3 (as fulfilled by using one of the presumptions of integrity).

[20] Section 31.1 of the *CEA* sets out the evidential burden for authentication:

> **Authentication of electronic documents**
>
> **31.1** Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

[21] Since it is the prosecution that seeks to enter into evidence the Instagram communications, then the prosecution has the burden of proving authenticity. The evidentiary threshold for proving authenticity under section 31.1 is a threshold of some evidence to prove that the document is what it purports to be. It can be established by circumstantial as well as through direct evidence, all of which can be provided through the lay evidence of a person comfortable with Instagram messaging (see *Richardson v. R.*, 2020 NBCA 35 at paragraph 31, *R. v. C.B.*, 2019 ONCA 380 at paragraph 68 and *R v Durocher*, 2019 SKCA 97 at paragraph 52). At this stage, and based on the facts of this case, the authentication is to focus on whether the evidence is a screenshot or photo of the relevant Instagram communications that make up the charges before the Court. It does not need to focus on whether or not the content itself is correct or not.

[22] Once the electronic document is authenticated, then the Court must proceed to step 2, to apply the statutory "best evidence" provisions of the *CEA* which augments the process. This statutory rule is intended to help ensure that the electronic document accurately reflects the original information input into the computing device by its author.

[23] With respect to the facts before this Court, the best evidence provisions of the *CEA* can be established through the application of the presumptions of integrity as set out at section 31.3 of the *CEA* which reads as follows:

> **Presumption of integrity**
>
> **31.3** For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven
>
> (a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;
>
> (b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or
>
> (c) if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it.
>
> [Emphasis added]

[24] The presumption of integrity set out at section 31.3 indicates three ways integrity of the documents is proven, which, of course, can be rebutted by the opposing party. The focus is on the integrity of the document or the computer system, focussing on how the electronic document is recorded and stored. The presumptions are aimed at providing some assurance that there have been no changes to the information contained in the electronic document that might have occurred either from technical problems or from tampering.

[25] For the purpose of the facts before the Court, the presumption relied upon by the prosecution is paragraph 31.3(a) of the *CEA*. In order to rely upon the presumption at paragraph 31.3(a), the prosecution needs to prove that at all material times the devices where the electronic document was handled were operating properly. Once again, the evidentiary threshold is "evidence capable of supporting a finding" which is the lower threshold of "some" evidence.

Admissibility

[26] Although admissibility was not contested in the current case, it is important to keep in mind that pursuant to section 31.7 of the *CEA*, the evidentiary framework set out therein for authenticating electronic documents does not "affect any rule of law relating to the admissibility of evidence, except [for] the rules relating to authentication and best evidence" (see *Ball* at paragraph 68).

[27] Section 31.7 of the *CEA* states:

> **Application**

> **31.7** Sections 31.1 to 31.4 do not affect any rule of law relating to the admissibility of evidence, except the rules relating to authentication and best evidence.

[28] In other words, notwithstanding the fact that the Court finds that the electronic document is admissible in terms of its authenticity and integrity, the actual admissibility of the document as evidence in a court martial is dependent on the common law rules of evidence. Admissibility is determined based on the relevance of the evidence and its probative value versus prejudicial effect as well as any exclusionary rules that apply.

[29] For example, in a case of sexual assault, evidence of Instagram private messages are presumptively inadmissible where a complainant has a privacy interest in them. They may only be admitted after the successful filing of a section 276 application (commonly referred to as a *Seaboyer* application, *R. v. Seaboyer*, [1991] 2 SCR 577).

[30] In addition to authenticity, the admissibility of any texts, Facebook or Instagram messages into evidence will depend on the purpose for which the materials are tendered and the rules of evidence that govern them.

[31] Generally, relevant evidence in a court martial is admissible unless it is subject to an exclusionary rule or its prejudice outweighs its probative value. In this case, the exclusion of the evidence would be "fatal to the prosecution's case", and the evidence has "real probative evidence" of high reliability.

Analysis

[32] Together, the three witnesses provided testimony as to how the Instagram communications were received and sent, who had access to C.L.'s Instagram account, how the communications between C.L. and "@randymanmax" were captured and recorded and who authored the various messages within the evidence sought to be introduced. C.L. testified as to the messages he authored and F.L. explained the messages that she sent out of C.L.'s account in what she described as an attempt to deter "@randymanmax". Both Constable Byrne and C.L. provided testimonial evidence of their understanding of how the messages were received and sent. In addition, F.L. who was unfamiliar with Instagram at the time, told the Court how she discovered the messages. She told the court she found them to be completely inappropriate and responded to some of the messages herself.

[33] In this case, expert evidence is not required to explain how everyday technologies such as Instagram messaging operates. The testimony of both Constable Byrne and C.L., both testifying as lay witnesses, demonstrated their familiarity with the program and its use and gave the required testimony (see *R. v. K.M.*, 2016 NWTSC 36 at paragraphs 12-15, 40-44; *R. v. Soh*, 2014 NBQB 20 at paragraph 27; "David M. Paciocco, "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (2013) 11: 2 CJLT at paragraphs 184-186, 188, 198, 211).

[34] Constable Byrne testified that the Instagram messages he viewed and took photos of were exactly the ones presented into evidence. All three witnesses testified that the content of the Instagram direct messages was accurate and that there was no appearance of alteration or tampering with the Instagram messages. Their explanations on how the Instagram messages were

recorded from C.L.'s IPad and stored raised no concerns. Given Constable Byrne's own familiarity with Instagram messaging, the Court can infer that the photos had not been tampered with. I am satisfied that the testimony of the three witnesses has provided some evidence capable of supporting the conclusion that the Instagram direct messages are what they are purported to be.

[35] As to the second part of the section 31.1 requirements permit the reliance on the presumption set out in section 31.3(a), there must be no other reasonable grounds to doubt the integrity of the electronic document system.

[36] Defence raised a concern that the Instagram communications tendered as evidence were captured by Constable Byrne taking photos of each page of the communications which he argued was equivalent to a cut and paste of evidence. Relying upon the Ontario case of *Donaldson*, he argued that the process of taking these photos was akin to cutting and pasting of a "conversation" which the court in *Donaldson* found did not meet the requirements of electronic documents. However, in the case of *Donaldson*, the evidence was rejected because there was no proof that it was an accurate "copy" of what was written. "[It was] clearly a cut-and-paste document, probably secured by using cut-and-paste functions on a computer." (see *Donaldson* at paragraph 13) Importantly, the evidence in *Donaldson* was rejected for a number of other reasons, mostly because there was no evidence tendered as to how the document was effectively generated and it did not meet the definition of "electronic document"

[37] Screenshots or photos of Instagram direct messages can originate electronically, but they are copies of original communications. Because the conversation occurred via Instagram direct messaging, it necessarily took place in a written form. The photos are simply a copy of the pre-existing written record and they do not create a separate record similar to the cut-and-paste document in *Donaldson*. In this case, Constable Byrne testified that he took photos of each page of the Instagram communications and then uploaded them into one document that was preserved in the police evidence management system. The photos simply created a copy of the pre-existing written record. In *Richardson*, the court found that a photocopy printout of a conversation could satisfy the best evidence rule. At paragraph 45 of *Richardson*, the court noted that it was the integrity of the data that was the focus of the inquiry and not how the data is displayed.

[38] I see no relevant difference in the fact that Constable Byrne preserved the conversations by taking a photo of them rather than using a computer to print them or tendering a phone or laptop with the conversations open and visible (see *R. v. Mills*, 2019 SCC 22).

[39] The testimonial evidence suggests that the photos preserved the written exchanges between C.L. and the Instagram account of @randymanmax and they are in what appears to be a complete and accurate format. Although C.L. deleted his Instagram account which was the original record of the Instagram messages through which the Instagram account of @randymanmax chose to communicate with him, all three witnesses testified that the record was a complete and accurate reflection of the conversations.

[40] After hearing the testimony of the witnesses, I am of the belief that the evidence as a whole proved the photos taken accurately depict the Instagram messages exchanged. There was

no evidence presented to doubt the integrity of C.L.'s IPad, Constable Byrne's IPhone 7 or the police evidence management system. There is some evidence capable of supporting a finding that the devices by or in which the electronic documentation was recorded or stored were operating properly.

[41] While defence did take issue with whether Master Sailor Machtmes authored the Instagram messages, he did not present any direct or circumstantial evidence that the messages were either altered or tampered with or that the posts had been changed in any way that interfered with the integrity of their contents. Master Sailor Machtmes did not testify. In other words, he did not advance any "evidence to the contrary" that is necessary to rebut the presumption of integrity set out in paragraph 31.3(a) of the *CEA*. However, defence did rely upon suggested inconsistencies in the prosecution's own evidence to question the accuracy of the document. He argued that because C.L. deleted his Instagram account, the Court cannot verify the accuracy.

[42] In short, defence raised concerns regarding the consistency of the communications and suggested that there appeared to be some messages which are out of context, suggesting that some texts are missing. He suggested that the inconsistency of the texts is some evidence of a problem.

[43] For example, defence points out that at page 7, it starts with, "Ok. We're you doing arms?" He highlights that at the bottom of the previous page the message from C.L. does not relate to this. Similarly at page 12 and 13, he submitted the transition between the pages suggests something is missing. Similarly, at page 13, defence counsel indicates there is no reference to asking for new blades so he does not understand the context.

[44] Defence counsel submitted that at pages 27, 28, 34, 37, 39, 40, 45, 47, 48, 60, 96 of the communications, there appears to be text missing in the various areas and he suggested that it raises the question of what else is missing. In some cases, he suggests that the flow just does not make sense. In explaining the way Instagram works, both C.L. and Constable Byrne explained how sometimes the texts were in response to a "story" item that had been posted by C.L. and could explain why some of the texts appear out of the blue and have less context as they are referring to a story item that C.L. had published.

[45] Further, in *Durocher*, at paragraph 84, the Saskatchewan Court of Appeal set out the process that should unfold when there are concerns for the accuracy of the data:

> [84] That said, authentication does not necessarily mean the document is genuine: "That is a question of weight for the fact-finder which often turns on determinations of credibility" (citations omitted, *Ball* at para 70). Evidence can be *authenticated* even where there is a contest over whether it is what it purports to be. As Professor David Paciocco (as he then was) explained in his article cited above, "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (December 2013) 11 Can J L & Tech 181 ["Proof and Progress"], this is not because the law is interested in false documentation (at 197):
>
> > It is simply that the law prefers to see disputes about authenticity resolved at the end of a case, not at the admissibility stage. Disputes over authenticity tend to turn on credibility, and credibility is best judged at the end of the case in the context of all of the evidence.

> "Authentication" for the purposes of admissibility is therefore nothing more than a threshold test requiring that there be some basis for leaving the evidence to the fact finder for ultimate evaluation. In *R. v. Butler*, [2009 ABQB 97] 2009 CarswellAlta 1825, [2009] A.J. No. 1242 (Alta. Q.B.), for example, the Court recognized where there was a live issue about whether the accused generated the Facebook entries in question that would be for the jury to decide.
>
> [Italics in original; underlining my own.]

[46] As Hoegg J.A. concluded at paragraph 51 of *R. v. Martin*, 2021 NLCA 1, the test to determine that an electronic document is admissible does not mean that it is what it appears to be:

> [51] As referenced above, authentication of electronic evidence does not prove that the electronic evidence is what it appears to be. Electronic evidence, once admitted, is simply evidence, no more no less. It is able to be used in the same way any other piece of admissible evidence can be used. The weight given to it is a matter for a trial court to determine in its consideration of the totality of the evidence when coming to a final conclusion on a case. While an individual piece of evidence tending to show that an electronic document is what it purports to be may be so strong that it actually determines that the electronic document is what it purports to be, there is no requirement for the supporting evidence to be so strong in order to be admissible. In short, electronic evidence is what it is, and its value remains for the trial court to determine.
> [Emphasis in original omitted.]

[47] Further, the authentication of the electronic document sought to be admitted does not assess or determine concerns about whether or not Master Sailor Machtmes authored the messages. As the trial judge exercising the gatekeeper function at the threshold admissibility stage, this Court only needs to be satisfied on a balance of probabilities that the statements were made by Master Sailor Machtmes. The court is entitled to rely upon the circumstantial evidence set out in the *voir dire* to do so. There was sufficient evidence linking Master Sailor Machtmes to the "@randymanmax" Instagram account based on the various postings that were made, the descriptions set out in the Instagram account as well as the testimonial evidence provided (see paragraph 52 of *Durocher*). Defence concerns regarding authorship are best answered in reviewing the comments made in *Richardson* at paragraph 49 where the New Brunswick Court of Appeal confirmed that:

> It is authentication which is required to satisfy the statutory provisions, and the Crown merely needs to establish on a balance of probabilities that the accused was the author of the messages. The bar is low. It is better to leave ultimate authorship along with ultimate weight to be determined at the end of the trial once all evidence is in.

[48] Further, the testimony of the three witnesses provided the Court with the necessary assurance that the communications have not been changed due to any technical glitches or from tampering. Keeping in mind the low threshold required under the *CEA* to establish authenticity, I am satisfied that the Instagram messages are electronic documents within the meaning of the *CEA* and that they comply with the legislative framework for authentication and integrity as set out in the *CEA*.

[49] Given that the Court has found that the Instagram communications have been adequately authenticated based on the protocol set out within the *CEA*, this does not necessarily mean there

are no issues with their accuracy. As the SCC clarified in *R. v. Morris*, [1983] 2 S.C.R. 190 at paragraph 192, "the admissibility of evidence must not be confused with weight."

[50] Consequently, the concerns raised by the defence go to the question of how much weight is to be provided to the document. As such, it is for the panel in this case to make this determination. Similarly, with respect to the defence's concerns regarding authorship, it is also up to the panel to assess all the evidence and determine whether Master Sailor Machtmes was the author of the Instagram communications in question.

Decision

[51] I find that the two-step process set out within the *CEA* which applies, first, for authenticity under section 31.1 of the *CEA* and, secondly, for the best evidence rule under paragraph 31.3(a), has been met. As referred to earlier, the admissibility of the authenticated evidence was not contested.

[52] Based on the facts of this case, any issues related to inconsistencies identified by defence counsel do not go to their admissibility. It is for the trier of fact to decide how much weight to attribute to the exchanges themselves and if there are inconsistencies that appear in the thread of communications; these are to be brought to the attention of the panel to be considered by them in the determination of the weight to be afforded to the communications.

FOR THESE REASONS, THE COURT:

[53] **FINDS** that the Instagram messages are admissible at trial.

Dated this 17th day of May 2021, at the Asticou Centre, Gatineau, Quebec

"S. Sukstorf, Commander"
Presiding Judge

Counsel:

The Director of Military Prosecutions as represented by Major M.-A. Ferron, Counsel for the Applicant

Lieutenant-Colonel D. Berntsen, Defence Counsel Services, Counsel for Master Sailor R.D. Machtmes, Counsel for the Respondent