IN THE COURT OF APPEAL

OF NEWFOUNDLAND AND LABRADOR

Citation: *R. v. Martin*, 2021 NLCA 1
Date: January 4, 2021
Docket Number: 201901H0008

BETWEEN:

HER MAJESTY THE QUEEN — APPELLANT

AND:

EDWARD MARTIN — RESPONDENT

Coram: Hoegg, Goodridge and Butler JJ.A.

Court Appealed From: Provincial Court of Newfoundland and Labrador
St. John's

Appeal Heard: November 6, 2019
Judgment Rendered: January 4, 2021

Reasons for Judgment by: Hoegg J.A.
Concurred in by: Goodridge J.A.
Dissenting Reasons by: Butler J.A.

Counsel for the Appellant: Sheldon B. Steeves
Counsel for the Respondent: Susan Day

Hoegg J.A.:

INTRODUCTION

[1] This case concerns the admissibility into evidence of screenshots depicting what purport to be posts from Edward Martin's Facebook.

[2] Mr. Martin was charged with (1) being in possession of a knife for a purpose dangerous to the public peace; (2) being in possession of a rifle for a purpose dangerous to the public peace; and (3) uttering a threat to members of the Royal Newfoundland Constabulary.

[3] At trial, the Crown sought to tender into evidence printouts of six screenshots depicting what appear to be posts from Mr. Martin's Facebook. A blended *voir dire* respecting their admissibility was held, after which the Judge excluded the evidence. The exclusion of the screenshot evidence caused the Crown's case respecting the rifle and threat charges to collapse. Mr. Martin was convicted of the weapon charge respecting the knife, which had been found on his person and which was not related to the screenshot evidence, but acquitted of the other two charges.

[4] The Crown appeals the Judge's decision to exclude the screenshot evidence.

BACKGROUND

[5] On March 27, 2018, Constable Park and Constable Kirby of the Royal Newfoundland Constabulary were dispatched to the residence of Mr. Martin to investigate a complaint of a domestic disturbance. When they arrived, they found that two other RNC officers had already been there. Constables Park and Kirby entered the residence, which was occupied by Mr. Martin and his girlfriend, and determined that the complaint needed no further investigation.

[6] The following night police received a tip that Mr. Martin had posted pictures and words on Facebook that suggested that he was going to harm police. The source of the tip wished to remain anonymous. Shortly after receiving the tip, two different police officers, Constable Smith and Constable Walsh, attended at Mr. Martin's residence to investigate it. Mr. Martin answered the door and became upset that the police had come to his home. He complained that they had been there the previous night for no reason, and told them to get off his property before closing and locking his door.

[7] The officers returned to the detachment where Constable Walsh attempted to access Mr. Martin's Facebook. He was unable to do so, so he contacted the source of the tip and requested that the Facebook postings be emailed to him. Six screenshots of what appear to be posts from Mr. Martin's Facebook were subsequently emailed to Constable Walsh. At the *voir dire* he described what the screenshots depicted.

[8] The first screenshot is a picture of a man kneeling back on to the camera with what appears to be the butt of a gun on the floor in front of him. The words "Ed's Post" appear over the picture. The screenshot is addressed to Jason Walsh and dated as sent to him on "Thursday, 3/29/2018 at 12:26 a.m."

[9] The second screenshot depicts a man whose face is partially covered and who is standing holding a gun pointed in the direction of the camera. The words "Ed's Post" appear over the picture. The screenshot is addressed to Jason Walsh and dated as sent to him on "Thursday, 3/29/2018 at 12:27 a.m."

[10] The third screenshot is composed of five pictures. The first is of a masked man wearing a red jacket and pointing a gun away from the camera. The second picture depicts Mr. Martin holding a long gun pointed toward the ceiling. The third picture depicts Mr. Martin holding a rifle. What is depicted in the fourth picture is not identifiable. The fifth picture depicts a kneeling man who appears to be the same person depicted in the first screenshot. The words "Ed Martin added 14 new photos" and "told U I ain't joking. Walk into my house again pigs" appear over the pictures. The screenshot is addressed to Jason Walsh and dated as sent to him on "Thursday, 3/29/2018 at 12:51 a.m."

[11] The fourth screenshot depicts a masked man wearing a red jacket holding a firearm with the butt facing up. The words "Ed's Post" appear over the picture. The screenshot is addressed to Jason Walsh and dated as sent to him on "Thursday, 3/29/2018 at 12:26 a.m."

[12] The fifth screenshot is of Mr. Martin pointing a firearm toward the ceiling. The words over the picture read "Ed's Post." The screenshot is addressed to Jason Walsh and dated as sent to him on "Thursday, 3/29/2018 at 12:49 a.m."

[13] The sixth screenshot depicts a picture of a masked man wearing a red jacket, a red hat, and jeans, pointing a firearm away from the camera. The picture appears under the words "Ed Martin added 4 new photos." The

screenshot is addressed to Jason Walsh and dated as sent to him on "Thursday, 3/29/2018 at 12:21 a.m."

THE *VOIR DIRE*

[14] The Crown called ten witnesses on the blended *voir dire*, all of whom were police officers.

[15] The officers who testified were all involved in the investigation of the complaint. Their evidence connected the screenshots to what they had witnessed or observed during their respective involvement in the investigation. Constables Park and Kirby, who had attended at Mr. Martin's residence on March 27, 2018, identified the room depicted in the Facebook posts as a room in Mr. Martin's residence by virtue of recognizing a picture on the wall of a man holding a baby and a bicycle leaned up against a wall of the room. Constable Park also testified that the colour of the walls of the room in Mr. Martin's house was the same colour as the colour of the walls of the room depicted in the Facebook posts.

[16] Constable Knight testified that he saw a person wearing a red baseball hat and a black hoodie leave Mr. Martin's residence on March 30, 2018. He notified other officers who came to the scene, recognized Mr. Martin, and arrested him. Constable Knight also spoke with Mr. Martin's girlfriend whom he observed climbing out of a back window of Mr. Martin's residence.

[17] Constable Walsh testified that he received the screenshots by email and that the copies before the Court were the same as he received. He said that he was familiar with Facebook and that he believed the screenshots to be photos of Facebook posts. He described each of the six screenshots and identified Mr. Martin as the unmasked man in the third and fifth screenshots. Constable Walsh testified that he received the screenshots from the person who did not wish to be identified approximately three hours after the times stated on the various postings.

[18] Constable Stuckless and Sergeant Soo testified that they were present when police conducted a search of Mr. Martin's residence on March 20, 2018. Constable Stuckless said she was present when a bag containing seven rounds of 7.62 ammunition was found inside Mr. Martin's residence and Sergeant Soo testified that he saw a pair of red sneakers in Mr. Martin's bedroom which appeared to be the same sneakers worn by the masked man depicted in the

Facebook posts. No computer was found in the search of Mr. Martin's residence.

[19] Corporal Stewart, who was qualified to give expert opinion evidence on the classification and identification of firearms, testified that she believed the rifle depicted in the Facebook posts to be a Soviet-style rifle with a swapped out stock and that the 7.62 ammunition found in Mr. Martin's residence was compatible with use of that kind of rifle.

[20] Mr. Martin presented no evidence on the *voir dire*.

[21] The Judge refused to admit the screenshot evidence saying:

> … the complainant who provided the alleged Facebook postings to Constable Walsh wished to remain anonymous and did not participate in the proceedings. Evidence of the screenshots were presented through Constable Walsh, who could not authenticate them or offer any information regarding their veracity, other than to confirm that they were the same postings that had been forwarded to him by email. Furthermore, there was no evidence to substantiate that Mr. Martin had a Facebook account, who would have access to that account, or whether the postings could only have been made by Mr. Martin. In the result, no witness testified to confirm that the alleged postings were found on an authentic Facebook account, no evidence was [adduced] that Mr. Martin was the author of the postings, no one testified that the postings were unaltered or unchanged, no computer was seized from Mr. Martin's apartment during the search warrant being executed so that that computer could be analyzed, and no weapon was found on the premises.

(Page 16 of the transcript of the Judge's oral decision)

ISSUE

[22] The issue on appeal is whether the trial Judge erred in excluding the screenshot evidence. Resolution involves determining whether the screenshot evidence was authenticated so as to meet the test for admissibility. Though not the primary focus of the appeal, resolution also requires addressing the issue of the integrity of the electronic system on which the evidence was stored. If this Court determines that the Judge ought to have admitted the screenshot evidence, the Crown asks the Court to rule on the use that a court could make of it at trial.

The Crown's Position

[23] The Crown acknowledges that the screenshot evidence must be authenticated to be admissible, and argues that the evidence it tendered on the *voir dire* provided the necessary authentication. The Crown says the Judge

erred by ignoring or discounting its evidence and effectively reasoning that authentication had to come from the anonymous person who actually saw the posts on Mr. Martin's Facebook.

Mr. Martin's Position

[24] Mr. Martin's position is that the screenshot evidence was not authenticated, and the Judge was correct to refuse to admit it. He argues that there was no witness who provided direct evidence that the screenshots depicted posts from a Facebook account belonging to him. He further argues that the Crown did not prove an absence of intention to mislead or that the images had not been altered before they came into Constable Walsh's possession.

ANALYSIS

The Law

[25] Facebook posts have been ruled by Courts to be electronic evidence (*R. v. Hirsch*, 2017 SKCA 14 at para. 24, *Richardson v. R.*, 2020 NBCA 35 at para. 22; *R. v. Ball*, 2019 BCCA 32 at para. 67; and *R. v. Durocher*, 2019 SKCA 97 at para. 77), and they fall within the definition of electronic documents in section 31.8 of the *Canada Evidence Act*, R.S.C. 1985, c. C-5 (the "*Act*"). Accordingly, they are data that has been recorded on a computer system, medium, or similar device which can be read or perceived by a person, computer system, or other device. They originate and are stored electronically.

[26] Screenshots of purported Facebook postings also originate electronically. However, they are simply copies of other material (*R. v. Mills*, 2019 SCC 22).

[27] In *Mills*, the Supreme Court of Canada considered whether screenshots of a conversation captured on the computer program "Snagit" were admissible evidence in a child luring trial. The appellant argued that a child luring conversation captured on Snagit was inadmissible because the capturing of it on Snagit violated the search and seizure provisions of section 8 of the *Charter*, which had the effect of making the otherwise admissible conversation inadmissible. The Supreme Court disagreed, ruling that the screenshot of the conversation captured by Snagit was simply a copy of the preexisting written record of the conversation. At paragraph 56 Karakatsanis J. explained:

> … I cannot see any relevant difference in the state preserving the conversations by using "Snagit" to take screenshots of them, than by using a computer to print them, or by tendering into evidence a cellphone or laptop with texted conversations open and

> visible. Ultimately, the "Snagit" screenshots are just a copy of the written messages. This use of technology is not intrusive or surreptitious state conduct.

[28] The Supreme Court determined that nothing turned on the use of a screenshot to capture the conversation, and because the conversation captured on the screenshot was admissible, the screenshot of the conversation was admissible. Justice Karakatsanis went on to say that "as technology evolves, the ways in which crimes are committed – and investigated – also evolve" and that interpretation of the "right to be secure against unreasonable search and seizure must keep pace with technological developments" (*Mills*, at para. 39). In regard to the role of screenshots, David Paciocco's words in "*Proof and Progress: Coping with the Law in a Technological Age*" (2013), 11 C.J.L.T. 181 at 183 are apt. He said:

> Fear of what is new cannot be allowed to impede the incorporation of newer technologies. After all, law is a practical discipline and it functions in the real world. It would be unrealistic to reject electronic documents and emails, notwithstanding realistic fears of ease of manipulation.

[29] Likewise in this case, the screenshots are simply copies of what appear to be posts from Mr. Martin's Facebook. The fact that the purported Facebook posts were captured in screenshots and tendered as such, in the absence of credible evidence that screenshot technology could have or did alter the Facebook posts depicted in the screenshots, is immaterial. What requires authentication are the Facebook posts depicted in the screenshots, which appear to be posts from Mr. Martin's Facebook.

[30] Authentication of Facebook posts, or screenshots of Facebook posts, being electronic documents, is governed by the common law principles of evidence and by the provisions of section 31.1 of the *Act*. In *Hirsch*, the appellate Court stated that the provision of the *Act* respecting the authentication of electronic documents is simply a codification of the common law (at para. 18), and in *R. v. C.B.*, 2019 ONCA 380, the Ontario Court of Appeal intimated the same (at para. 57). In *The Law of Evidence*, 8th edition, (Toronto: Irwin Law Inc., 2020) David M. Paciocco, Palma Paciocco, and Lee Stuesser, the authors write that the authenticity requirement found in section 31.1 of the *Canada Evidence Act* is indistinguishable from the common law authenticity standard (at 563). In this regard, I note section 31.7 of the *Act*, which states: "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" which I interpret to mean that the provisions of sections 31.1 to 31.4 of the *Act* do not affect the common-law rules relating to the admissibility of evidence,

specifically, relevance, exclusionary rules, and the probative value versus prejudicial effect analysis.

[31] In any case, the threshold for admissibility of authenticated electronic documents is low, which is in keeping with the general principle that relevant evidence in a criminal trial is admissible unless it is subject to an exclusionary rule or its prejudice outweighs its probative value. In *C.B.*, the Court described the common law requirement for authentication of real or documentary evidence as requiring the introduction of some evidence that the item is what it purports to be, and stated… "[t]he requirement is not onerous and may be established by either or both direct and circumstantial evidence" (at para. 66).

[32] *C.B.* concerned whether electronic evidence consisting of screenshots of text messages between the accused and the complainant were admissible evidence. The trial judge refused to admit the screenshot evidence because in his view the messages were not authenticated. The accused was convicted. He appealed his conviction arguing that the trial judge erred by not admitting the screenshot evidence which was important to his defence.

[33] On appeal, the Ontario Court of Appeal described authentication and how it can be established:

> 65 Authentication is the process of convincing a court that a thing matches the claim made about it. In other words, it is what its proponent claims it to be. Authentication is intertwined with relevance: in the absence of authentication, the thing lacks relevance unless it is tendered as bogus. Thus, authentication becomes necessary where the item is tendered as real or documentary evidence.
>
> …
>
> 67 For electronic documents, s. 31.1 of the *CEA* assigns a party who seeks to admit an electronic document as evidence the burden of proving its authenticity. To meet this burden, the party must adduce evidence *capable* of supporting a finding that the electronic document is what it purports to be. Section 31.8 provides an expansive definition of "electronic document", a term which encompasses devices by or in which data is recorded or stored. Under s. 31.1, as at common law, the threshold to be met is low. When that threshold is satisfied, the electronic document is admissible, and thus available for use by the trier of fact.

[34] With respect to Section 31.1 of the *Act*, the appellate Court confirmed the modest threshold for authentication, and stated at paragraph 68:

> 68 To satisfy this modest threshold for authentication, whether at common law or under s. 31.1 of the *CEA*, the proponent may adduce and rely upon direct and

> circumstantial evidence. Section 31.1 does *not* limit how or by what means the threshold may be met. Its only requirement is that the evidence be *capable* of supporting a finding that the electronic document "is that which it is purported to be." That circumstantial evidence may be relied upon is well established: *Hirsch*, at para. 18; *R. v. Colosie*, 2016 ONSC 1708 (Ont. S.C.J.), at para. 25; *R. v. Bulldog*, 2015 ABCA 251, 326 C.C.C. (3d) 385 (Alta. C.A.), at para. 35; see also *R. v. Evans*, [1993] 3 S.C.R. 653 (S.C.C.), at p. 663. This accords with general principles about proof of facts in criminal proceedings, whether the facts sought to be established are preliminary facts on an admissibility inquiry or ultimate facts necessary to prove guilt.

[35] The Court then discussed the evidence pertinent to that appeal, including the complainant's denial that she had been texting with the accused, and concluded that the text messages captured in the screenshots were authenticated by other circumstantial evidence, making them admissible. The Court set aside the conviction, and ordered a new trial to include the evidence respecting the texts.

[36] In *Richardson*, the issue was whether the trial judge erred in admitting a series of MSN text messages which appeared to be messages between the complainant and the accused and which had been stored in a computer. The accused had argued at trial that the text messages were not messages from him to the complainant, but messages he sent to a different man who was his boyfriend at the time. The complainant and other witnesses testified that the content of the messages was accurate to the best of their recollections (they had not seen them for several years), and their explanations of how the messages had been stored raised no concern. The Court was satisfied that the electronic evidence was authenticated, and admitted it into evidence. The accused was convicted. He appealed.

[37] The New Brunswick Court of Appeal upheld the trial judge's admissibility ruling. In doing so, the Court stated that the threshold for evidence capable of supporting what is sought to be admitted is low, and that it can be met by evidence from which a judge can reasonably find the document to be what it purports to be (at para. 27).

[38] In *Hirsch*, the question was whether screenshot evidence of Facebook posts on which the judge relied to support his conviction of the accused was authenticated. The Facebook posts depicted nude photographs of the complainant. She had received the screenshots of the posts from a friend who did not testify at the trial. The trial judge relied on the screenshot evidence in convicting the accused. The accused appealed, arguing that the screenshot evidence had not been authenticated.

[39] The Saskatchewan Court of Appeal upheld the trial judge's ruling on admissibility. In so doing, the Court stated that authentication in section 31.1 of the *Act* is not an onerous requirement, and quoted with approval *Watt's Manual of Criminal Evidence, 2016* (Toronto: Thomson Reuters, 2016) at 1115:

> The *burden* of providing authenticity of an electronic document is on the person who seeks its admission. The *standard* of proof required is the introduction of evidence *capable* of supporting a finding that the electronic document is as it claims to be. In essence, the threshold is met and admissibility achieved by the introduction of *some* evidence of authenticity.
>
> (Emphasis in original.)

[40] The Court reviewed the complainant's evidence that she recognized the content of the Facebook posts and her explanation as to why she recognized the posts. The Court found that her evidence authenticated the Facebook posts despite the facts that she had not received the screenshots directly or that she had not viewed the posts herself on the accused's Facebook, and that the person who had sent her the screenshots did not testify.

[41] In *Durocher*, the issue was whether screenshots of Facebook conversations between the accused and the complainant were authenticated. In finding that the screenshot evidence had been authenticated, the Saskatchewan Court of Appeal ruled that the threshold for admissibility is low, and that once admitted, evidence is available for use by the trier of fact. The Court went on to explain that the admissible screenshot evidence was still subject to evaluation by the Court:

> 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.

[42] The Ontario Court of Appeal again considered authentication of electronic documents in *R. v. Farouk*, 2019 ONCA 662. In *Farouk*, the electronic documents in question were website contents offering "body rub services", including a contact telephone number that matched the telephone number on the accused's cell phone records. The trial judge ruled the evidence inadmissible on the basis that the prejudicial effect of the sexually explicit website material outweighed its probative value. On appeal, the offender argued, among other grounds, that the website contents, as electronic documents, had not been authenticated. The Court of Appeal disagreed, saying that the investigating officer's testimony connecting the accused's telephone number to the website was a sufficient basis upon which to authenticate the website evidence for the purposes of admissibility:

> 60 Even if the website contents were to be construed as real evidence actually adduced at trial, the investigating officer's testimony would appear sufficient for the purpose of authentication. The threshold for authentication of evidence, both at common law and under s. 31.1 of the *Canadian Evidence Act*, is modest: there must be evidence that is capable of supporting a finding that the electronic document "is that which it is purported to be": *R. v. C.B.*, 2019 ONCA 380 (Ont. C.A.), at para. 68. Both circumstantial and direct evidence may be relied upon for this purpose: *C.B.*, at para. 68. Here, the investigating officer described her "Google" search for the "647" number and the website in general terms. In the circumstances, this would have been sufficient for the purpose of authentication. In light of the appellant's concession at trial that the telephone number to which he sent text messages was associated with the website for the body rub service and the operation of that business, no further authentication was required in any event.

[43] In summary, common law principles respecting admissibility of evidence and the provisions of the *Act* govern the admissibility of electronic documents. Authentication of electronic documents for the purpose of admissibility under section 31.1 is established by meeting the low standard of "some evidence of the tendered document is what purports to be".

Application of the Law to this Case

[44] The Crown agrees that it had the burden to authenticate the purported Facebook posts, and argues that the evidence it called on the *voir dire* did so.

[45] As part of its argument, the Crown maintains that the Judge effectively decided that the person who provided the screenshots to Constable Walsh had to

authenticate the Facebook posts, and because that person did not testify, the evidence was not authenticated. I agree that the Judge determined that the Facebook posts were not authenticated, but I do not agree that she effectively decided that the person who sent the screenshots to Constable Walsh had to provide authentication. The Judge's statement in her decision that "Constable Walsh could not authenticate the screenshots" *implies* that she appreciated that authentication evidence could come from a witness other than the anonymous person who sent the screenshots to Constable Walsh. However, the Judge's decision does show that she effectively required direct evidence from a witness who could testify to having seen the posts on Mr. Martin's Facebook, in order to authenticate the Facebook posts. She did not consider whether the circumstantial evidence which the Crown submitted could authenticate the Facebook posts. It is an error in principle to fail to consider relevant evidence material to a core issue.

[46] Evidence respecting authentication at common law or under section 31.1 of the *Act* can be established by circumstantial as well as by direct evidence (*C.B.*, at para. 68; *Farouk*, at para. 60; and *Durocher*, at para. 52). There is no requirement that authentication evidence be restricted to direct evidence. Circumstantial evidence can be good evidence in authentication inquiries just as it is in other judicial proceedings.

[47] The wording of section 31.1 of the *Act* must also be considered. It stipulates that there must be evidence *capable of supporting a finding* that the electronic evidence sought to be admitted is what it purports to be. The section does not require a determination that the electronic evidence is in fact what it purports to be. Evidence "capable of supporting" a finding is quite different from evidence "determining" or "capable of determining" a finding. In other words, the evidence only needs to assist the trier of fact in determining whether the electronic document is what it purports to be. Moreover, as the Court in *C.B.* noted, section 31.1 does not limit how or by what means the threshold may be met (at para. 68). Neither does it impose a particular standard for threshold admissibility of electronic evidence. What is required is only some evidence that is logically probative of whether the electronic document is what it purports to be. Whether the electronic document will be relied on is a matter for the judge in weighing and balancing all of the admissible evidence and finally determining the case.

[48] In this regard, I refer to the Supreme Court of Canada's decision in *R. v. Morris*, [1983] 2 S.C.R. 190 wherein the Court stated: "the admissibility of

evidence must not be confused with weight" (at 192) and then further explained the fundamentals of the admissibility of evidence (at 201):

> (1)… nothing is to be received which is not logically probative of some matter requiring to be proved; and (2) that everything which is thus probative should come in, unless a clear ground of policy or law excludes it"

The Court added that admissibility of evidence is also subject to the discretionary power of judges to exclude logically probative evidence:

> …as being of too slight a significance, or as having too conjectural and remote a … connection; … as being too dangerous in their effect on the jury… and as being impolitic, or unsafe on public ground, others, on the bare ground of precedent.

[49] As noted above, authentication does not mean the document is genuine. If the "evidence capable of supporting" a finding had to actually determine that the electronic document is in fact what it purports to be, a court would always be required to subject individual pieces of electronic evidence to the standard of beyond a reasonable doubt or the balance of probabilities at the admissibility stage. Such a requirement conflicts with general evidentiary principles respecting the admissibility of evidence. There is no requirement that individual pieces of evidence (in this case an electronic document) be subjected to the standard of proof of beyond a reasonable doubt or the balance of probabilities during the trial process. There is no requirement in criminal cases (*R. v. Morin*, [1988] 2 S.C.R. 345 (S.C.C.) at 354; and *R. v. J.M.H.*, 2011 SCC 45, [2011] 35 S.C.R. 197 (S.C.C.) at para. 31). Neither am I aware of any evidentiary principle requiring that evidence be admitted only if it is proved to be actually true or reliable. The truth and reliability of individual pieces of evidence is left to the judge's weighing and evaluating in the context of all of the evidence in making the final determination. In short, a piece of electronic evidence does not have to meet an additional standard of proof like the balance of probabilities or beyond a reasonable doubt in order to be admitted into evidence. Individual pieces of evidence tendered in a trial are admitted on the basis of relevance to a fact in issue, subject to exclusionary rules and the prejudice versus probative value inquiry.

[50] Electronic evidence is intangible evidence and its type and use are continuously evolving in our present world. Perhaps because of these factors, the *Act*, which has been held to be a codification of the common law, imposes the specific requirement that there must be some evidence capable of supporting a finding that the electronic document is what it appears to be before it is admitted. Section 31.1 is silent as to the effect of evidence tending to show that

the document is not what it appears to be. If there is evidence capable of supporting a finding that the document is not what it appears to be, the document could still be admissible and the weight to be given to the document, if any, would be sorted out in the final analysis of the evidence by the trial judge. Admissibility of electronic evidence remains governed by general evidentiary principles, which in this case is simply that there be some relevant evidence of probative value to support a finding that the electronic document 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.

[52] In this case the circumstantial evidence supporting authentication was considerable. Police officers familiar with Facebook testified that the purported posts had the same format and design as Facebook posts. Various police officers were able to identify Mr. Martin in two of the pictures depicted in the Facebook posts. Pictures depicting Mr. Martin holding a long gun, in the context of the content of the posts, is relevant circumstantial evidence of his personal involvement in the Facebook posts and as such, is capable of supporting a finding that the posts are from his Facebook. Also relevant circumstantial evidence is the officers' identification of the room in the pictures as a room in Mr. Martin's residence, along with several of the items in the room, and as such are circumstantial evidence of Mr. Martin being in his residence when he posed for the posts. The words "Ed's Posts", "Ed Martin posted", "Ed Martin added 14 new photos" and "Ed Martin added four new photos" appear variously above the posts. This is also relevant circumstantial evidence that the posts came from Mr. Martin's Facebook. The ammunition found in the search of Mr. Martin's residence was the type used with the firearm depicted in the posts, and the times noted on the various posts are very close to the times of Mr. Martin's interaction with the police, making the postings consistent with the temporality of his grievance with police and possible motivation to take action.

All of this circumstantial evidence is relevant and probative of some elements of the offence with which Mr. Murphy was charged and supports a finding that the Facebook posts are what they purport to be. This is not to say that this circumstantial evidence constitutes proof of Mr. Martin's guilt. It is only to say that authentication of the screenshots was established for the purposes of threshold admissibility. Accordingly, the Judge erred in failing to consider the circumstantial evidence and finding that the screenshots were not authenticated.

[53] At this point I would be remiss if I did not note that authorship of a Facebook post is not the same thing as authentication. Authentication goes to admissibility, authorship is a question for ultimate determination. See paragraph 85 of *Durocher* for a discussion of these two distinct concepts.

[54] The focus of this appeal was on authentication of the Facebook posts, as that had been the focus of the *voir dire* at trial. The system integrity of the device on which the screenshots were stored does not appear to have been an issue at trial and section 31.2 of the *CEA* was not mentioned. On appeal, both the Crown and Mr. Martin referenced section 31.2 of the *CEA* in their factums, but system integrity and how the *CEA* provisions would apply to the within matter were not argued.

[55] Section 31.2 of the *CEA* is described as the best evidence rule, although it bears only a tenuous relationship to the common law best evidence rule, which concerns whether proffered documentary evidence, if not an original document, is in fact the best evidence that can be proffered. Rather, section 31.2 concerns the integrity of the system on which proffered electronic evidence has been stored, so as to address whether the proffered electronic document has been altered or tampered with in a way that affects its integrity (*The Law of Evidence*, at 564 and *Proof and Progress*, at 200).

[56] While section 31.2 does not expressly state that system integrity is an admissibility issue, this Court's recent decision in *R.* v. *Jennings*, 2020 NLCA 40 ruled that compliance with section 31.2 is an admissibility requirement (at paras. 13 and 14). Likewise, several of the cases referenced above which deal with authentication of electronic documents for the purpose of admissibility also treat the integrity of the system on which the tendered electronic document was recorded or stored as an admissibility consideration (*Richardson*, at para. 32; *Durocher*, at para. 91; and *Ball*, at para. 68).

[57] As indicated, the purpose of section 31.2 is to ensure that an electronic system which records or stores an electronic document does not alter, distort, or

manipulate the document such that its integrity, or what the document purports to be, is affected in a way that matters. When considering system integrity, the issue is not whether a judge has a vague unease about the possibility of any device on which the tendered document is recorded or stored having the potential to alter, distort, or manipulate the tendered document in any way. Rather, the issue is whether in an instant case, a court can have some level of assurance that the device which stored or recorded the document did not alter, distort, or manipulate the electronic document so as to affect the integrity of its contents. Such assurance is often obtained by hearing from witnesses who can attest to whether the content of a tendered electronic document has been altered or whether the system on which the document was stored was functioning properly (see *Hirsch*, *Richardson*, and *Durocher* as examples). When such witnesses are not available, like in the instant case, reliance on the presumptions set out in section 31.3 may obtain. The presumptions provide for the reception of relevant and reliable evidence in appropriate circumstances so that a court will not be deprived of relevant and reliable evidence.

[58] It is a very tall order for a tendering party to prove that every device which a tendered electronic document passed through did not have the potential to alter, distort, or manipulate the tendered document, when it passed through those devices to reach the recipient. To insist on this standard would require the tendering party to call expert evidence respecting every device and every iteration of the electronic document as it passed. Courts have rejected the requirement for expert evidence in this regard (see *Richardson*, at para. 31 and *R. v. Ball*, 2019 BCCA 32 at para. 69; 77). See also Professor Paciocco's discussion of the reliability of lay evidence at pages 185-186 of *Proof and Progress*. In any event, satisfaction of the best evidence rules respecting electronic documents as found in sections 31.2 and 31.3 of the *Act* must always focus on the integrity of the content of the tendered document.

[59] In this case, I am satisfied that of section 31.3(a) of the *Act*, provides assurance of system integrity for the purpose of admitting the screenshots into evidence.

[60] Section 31.3(a) provides that integrity is presumed when, in the absence of evidence to the contrary, there is evidence capable of supporting a finding that the devices by or in which the electronic document was recorded or stored were operating properly. As discussed above in relation to section 31.1 with respect to authentication, "evidence capable of supporting a finding" represents a low threshold which is met by some relevant evidence which could be used to support a finding of system integrity.

[61] The presumption in section 31.3(a) was considered by the Ontario Court of Appeal in *R. v. S.H.*, 2019 ONCA 669, aff'd 2020 SCC 3. In *S.H.*, data extracted from a cell phone, including text messages, was in the possession of the Crown but the witness who used the cell phone was not available. The integrity of the cell phone from which the electronic documents sought to be admitted were extracted was challenged. The appellate Court rejected the argument that it was necessary to call the owner of the phone to establish that at all material times the cell phone was operating properly, saying that was not required under section 31.3(a) (para. 28). The Court also rejected the argument that the Crown needed to adduce evidence that the phone had been tested to ensure that the text messaging function was operating properly:

[62] The Court ruled that the integrity of the cell phone from which they were sent was presumed by section 31.3(a), saying:

> 17 I accept the Crown's submission that the evidence adduced at trial was capable of supporting a finding that the Samsung cell phone was functioning properly at all material times or, it if was not, that any malfunction did not affect the integrity of the electronic documents relied on by the Crown, and that there are no other grounds to doubt the integrity of the electronic documents system. …
>
> …
>
> 25 In my view, the requirement in s. 31.3(a) of the *Canada Evidence Act* for "evidence capable of supporting" the relevant findings represents a low threshold. This is apparent when s. 31.3(a) is read in context with, for example s. 31.3(b), which requires that it be "established" that an electronic document was recorded or stored by a party adverse in interest.

[63] In short, the Court in *S.H.* confirmed that the threshold to be satisfied in order to rely on the presumption in section 31.3(a) is low, and that the language "evidence capable of supporting" in the subsection suggests that the same low threshold which applies to the authentication requirement found in section 31.1 applies in the context of system integrity under section 31.3(a).

[64] Professor Paciocco also addressed this low threshold and the evidence required to meet it in *Proof and Progress*. At page 205, he discusses evidence that would satisfy the presumption:

> If a witness provides evidence that an email or image <u>was received</u> on a device that functions as a computer…this is circumstantial evidence that the computer systems or other similar devices that sent or received the message were operating properly. <u>If that document is legible or readable and coherent this is some evidence that the integrity of the document was unaffected by any problems that may have affected the computer</u>

> system. […] Simple proof of the receipt of a coherent document should work with this background information to satisfy the basic fact required by this presumption.
>
> (Emphasis added)

[65] *Richardson* also addressed system integrity under section 31.2 and the presumption under section 31.3(a). The Court found that a photocopied printout of an MSN conversation could satisfy the best evidence rule and that photocopying the printout had no effect on the integrity of the data. In reaching this conclusion, the Court noted that it is the integrity of the data that is the focus of the inquiry, not how that data is displayed (para. 45). The Court rejected the notion that the electronic documents had to be produced by the person who owned the system on which the documents had originally been stored (para. 46). The Court also rejected the submission that the evidence must show that the electronic documents are totally identical to the data that was input into the electronic documents system, saying that this is not the standard required under the provisions of the *Act* (para. 47).

[66] In this case the fact that the "printout" of the screenshots the Crown sought to adduce did not come to Constable Walsh directly from the original system on which the electronic documents were stored, instead passing through the anonymous complainant's device from which the screenshots were sent to him, does not jeopardize system integrity. The screenshots in this case were simply a picture of the data, like in *Mills*, and like the photocopy in *Richardson*.

[67] In this case, Constable Walsh, the recipient of the screenshots, testified that the documents he viewed and downloaded were the same as the ones which had been emailed to him. He said that he was familiar with Facebook and that the structure and layout of the screenshots were entirely consistent with the Facebook model. Given his familiarity with Facebook and his evidence that the screenshots were consistent with Facebook, it can be inferred that the Facebook posts in the screenshots had not been altered. That alone is some evidence of system integrity for the purposes of admissibility under the section 31.3(a) presumption. As well, just as Constable Walsh was alive to whether his own system distorted or altered the Facebook posts, he also would have been alive to whether the complainant's system had altered or compromised the posts. Again, his evidence was that there was no appearance of alteration or tampering with the posts. To the extent that the integrity of the complainant's device is also an issue, Constable Walsh's evidence is also evidence that the integrity of the complainant's system did not alter, distort or manipulate the integrity of the Facebook posts. In my view, like Professor Paciocco said in *Proof and*

Progress, Constable Walsh's evidence was evidence that the screenshots were "legible or readable and coherent" and that the integrity of the content of the screenshots was unaffected by any problems respecting the operation of any computer system at play in the proceeding. Accordingly, Constable Walsh's evidence is therefore capable of supporting a finding of system integrity sufficient to satisfy the presumption of integrity found in section 31.3(a), provided the presumption is not rebutted by evidence to the contrary.

[68] In order to rely on the presumptions set out in section 31.3(a) there is the additional requirement that there be no other reasonable grounds to doubt the integrity of the electronic document system.

[69] Evidence to the contrary was considered by the British Columbia Court of Appeal in *Ball* where the admissibility of screenshots of Facebook messages pertaining to an arson case was in issue. While the Court did not determine whether the screenshots satisfied the best evidence rule, the Court did determine that, if the trial judge had properly scrutinized the screenshots, there was a realistic possibility that the judge would have excluded or limited their use. I note that in *Ball* there was evidence to the contrary that could rebut the presumption of integrity (para. 85), because the accused testified that his ex-girlfriend, who had been the Crown's only authenticating witness at trial, had tampered with the Facebook messages.

[70] In this case there was no evidence to the contrary. Mr. Martin did not testify on the *voir dire*. Neither he nor anyone else said that any person had tampered with any system on which the Facebook posts were recorded or stored, or that the posts had been altered so as to interfere with the integrity of their contents. In other words, Mr. Martin did not advance any "evidence to the contrary" that would rebut the presumption of system integrity found in section 31.3(a) of the *Act*.

[71] In the result, system integrity for the purposes of admissibility of the screenshots tendered by Constable Walsh was established. In arriving at this conclusion, I note and agree with the *Richardson* Court's comments that the presumption in section 31.3(a) can be satisfied by both circumstantial and direct evidence, and that lay evidence can satisfy the presumption (at para. 31). Likewise in this case, lay evidence from a person familiar with Facebook like Constable Walsh (as opposed to a Facebook expert) is satisfactory. I also agree with the above-referenced comments of Professor Paciocco in *Proof and Progress* to the effect that if the electronic document received is legible, readable, and coherent, this is some evidence that the integrity of the document

was unaffected by any problem the system that sent or received the electronic documents might have had. In this regard, I also note the comments in *Durocher* to the effect that integrity can be presumed to be established pursuant to either 31.3(a) or 31.3(b) unless there is credible evidence to suggest otherwise (para. 95). This result also accords with the fundamental rules respecting the admissibility of evidence, as discussed above in relation to authentication, as well as with the views expressed in other appellate cases that expert evidence is not required.

[72] As a final point respecting the admissibility of electronic documents pursuant to the provisions of the *Act*, I would echo the words of Justice Paciocco in *R. v. Donaldson*, [2016] O.J. No. 7153, 140 W.C.B. (2d) 513 at paragraphs 3 and 4:

> 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*. …
>
> … Their intention is to provide a generous gateway for a common form of communication in our current society, but at the same time to provide some degree of quality control, given the risks that many forms of electronic communication can be manipulated.

To Justice Paciocco's words I add that the provisions of the *Act* are not meant to be roadblocks to the admission of relevant and reliable evidence going to the core issues in a case.

[73] It is worth reiterating at this point that the admissibility of evidence does not determine authorship. That is, authentication of the electronic document and the presumption of system integrity do not determine concerns about whether it was in fact Mr. Martin who authored the Facebook posts. While this concern may impact other evidentiary principles, such as the relevance, reliability and ultimate weight to be afforded to the evidence, it does not affect the applicability of the section 31.3(a) presumption (see *Proof and Progress*, at 207) or authentication respecting admissibility of the screenshots.

[74] In the result, the judge erred in failing to admit the screenshots of the Facebook posts purporting to be from Mr. Martin's Facebook. The low threshold required by the provisions of the *Act* regarding authentication and system integrity was met for the purposes of admissibility.

What use can be made of the screenshots once admitted?

[75] The Crown asks what use can be made of the screenshot evidence in this case once it is admitted. This is an entirely different question than whether the evidence was admissible. The short answer is that once admitted, the trial judge can use the evidence the same way he or she would use any other evidence, meaning that the screenshots of the Facebook posts in this case are like any other evidence adduced in the case. In other words, a court could consider the Facebook posts along with all of the other relevant evidence in reaching a conclusion respecting whether Mr. Martin is guilty of the charge.

[76] The Judge's decision on the *voir dire* suggests that even if she had admitted the screenshot evidence, she would not likely have convicted Mr. Martin of the rifle and threat charges. The reasons she gave for not admitting the evidence suggest that she would not have been convinced of Mr. Martin's guilt beyond a reasonable doubt respecting those changes.

[77] It would be inappropriate for this Court to pronounce on whether the screenshot evidence could be relied on to convict Mr. Martin. That was and is the province of the trial court. Trials are fluid processes, and more evidence could be adduced. In any event, the use of the screenshot evidence by a trial judge would depend on his or her reasoned consideration of it within the totality of the evidence adduced at trial.

DISPOSITION

[78] In the result, I would allow the appeal and remit the matter to the Provincial Court for further proceedings at the call of the Crown.

_____

L. R. Hoegg J.A.

I concur: _____

W. H. Goodridge J.A.

Dissenting Reasons of Butler J.A.:

INTRODUCTION

[79] While I agree that the screenshots were electronic records, and that the relevant provisions of the *Canada Evidence Act* were required to be considered for their admission, respectfully I disagree with my colleagues on what was required to be established for threshold admissibility of the electronic records in this case.

[80] First, while I agree that the standard of proof for authenticity under section 31.1 of the *Act* is modest ("some evidence capable of supporting"), the focus of the inquiry must be upon what was captured in the screenshots, not the manner by which the evidence was captured.

[81] My colleague concludes that the officers' testimony "connected the screenshots to what they had witnessed or observed during their respective involvement in the investigation". Respectfully, I disagree because neither officer had ever observed the events depicted in the screenshots. The circumstantial evidence was sufficient to identify the apartment and Mr. Martin (in two screenshots) but not the event depicted.

[82] Secondly, this Court recently confirmed that establishing integrity is a second requirement for admissibility under the relevant provisions of the *Act (Jennings,* at para. 13). This is consistent with the view expressed by the New Brunswick, Saskatchewan, British Columbia and Ontario Courts of Appeal in *Richardson,* at para. 32; *Durocher*, at para. 91; *Ball,* at para. 68; and *S.H.,* at para. 10 respectively and the approach taken in *Hirsch,* which is consistent with proof of integrity being the second statutory requirement for admissibility of electronic records. I conclude that, on the facts, this second requirement could not be met.

[83] Finally, as recently addressed by this Court in *Jennings* (at paras. 14 and 17), section 31.7 affirms the requirement to consider (in addition to the *Act*'s provisions on authenticity and integrity) other common law and/or statutory rules relative to the particular character of the evidence (*The Law of Evidence in Canada,* at 1351-1356 citing *Saturley v. CIBC Worldmarkets Inc.,* 2012 NSSC 226, at paras. 11-13; *S.H.,* at para. 10). In this regard I adopt the approach endorsed in *Ball,* at para. 68, and applied in *R. v. Soh*, 2014 NBQB 20, at paras. 32-52; *R. v. J.V.,* 2015 ONCJ 837, at paras. 3 and 31-32; and *Durocher,* at paras. 68-73 which I discuss later herein.

[84] In this case, the evidence was in the nature of electronic documents as defined in section 31.8 but it was proffered for proof of the truth of the events depicted in the screenshots which were in the character of photographic reproductions. I conclude that this required consideration of the three-part test stated in *R. v. Creemer* (1967), 4 N.S.R. 1965-69 546, [1968] 1 C.C.C. 14 (N.S.C.A.) at 22 and that, without verification of the contents of the screenshots on oath by a person able to speak to their accuracy, the screenshots were inadmissible in this case.

[85] The trial judge was not referred to the relevant provisions of the *Act.* However, I conclude that application of these provisions and the *Creemer* test to the evidence yields the same result. I am of the view that threshold admissibility of the electronic records could not be established in this case.

[86] I would therefore have dismissed the appeal.

ANALYSIS

The Legislation

[87] The relevant provisions of the *Act* are stated in full below:

> 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.
>
> 31.2 (1) The best evidence rule in respect of an electronic document is satisfied
>
> > (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
> >
> > (b) if an evidentiary presumption established under section 31.4 applies.
>
> (2) Despite subsection (1), in the absence of evidence to the contrary, an electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.
>
> 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.
>
> 31.4 The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting
>
> (a) the association of secure electronic signatures with persons; and
>
> (b) the integrity of information contained in electronic documents signed with secure electronic signatures.
>
> 31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.
>
> 31.6 (1) The matters referred to in subsection 31.2(2) and sections 31.3 and 31.5 and in regulations made under section 31.4 may be established by affidavit.
>
> (2) A party may cross-examine a deponent of an affidavit referred to in subsection (1) that has been introduced in evidence
>
> (a) as of right, if the deponent is an adverse party or is under the control of an adverse party; and
>
> (b) with leave of the court, in the case of any other deponent.
>
> 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.

Authenticity

Standard of Proof

[88] I agree that the standard of proof for establishing authenticity under section 31.1 (“evidence capable of supporting a finding that the electronic

document is that which it is purported to be") is a modest threshold that may be met by either or both circumstantial or direct evidence (*C.B.,* at para. 68). However, as I explain later, the threshold for admissibility will depend upon where reliance is placed for establishing the second statutory requirement (integrity) and the effect of other common law and/or statutory rules required to be considered under section 31.7.

What is being Authenticated

[89] "In order to determine what needs to be authenticated, the purpose for which the evidence is presented has to be borne in mind" (*Donaldson,* at para. 6). In this case, the Crown's theory was that the Facebook posts depicting Mr. Martin holding a prohibited firearm and making a threat originated from his account.

[90] There was "some evidence capable of supporting" that the records were screenshots of a Facebook page that the police had received from an anonymous source. The police could identify Mr. Martin and his apartment in two of them. This was all that could be authenticated under section 31.1. In other words, the police testimony authenticated only the screenshots and not the event depicted in them (*The Law of Evidence,* at 560).

[91] The distinction I draw is apparent in the cases cited by the majority in the discussion of authentication. In each of *Mills, Hirsch, C.B., Richardson* and *Durocher,* there was a witness who could testify to what was captured in the electronic document because they had either seen the messages, or photographs, and/or had participated directly in the relevant conversation. In this case there was no witness who could do so.

Integrity

[92] " 'Integrity' is not defined [in the *Canada Evidence Act* provisions] but clearly refers to the ability of the system to record and store information accurately" (*Proof and Progress*, at 202). As previously stated, I accept that it is a second statutory requirement to admissibility of electronic records under the *Act.*

Purpose of Integrity

[93] I accept that the purpose of the integrity provisions is to ensure "that the information obtained from or displayed by the computer is the same information that was input" (*The Law of Evidence*, at 564; *Proof & Progress,* at 200) and

that they are "a generous gateway for a common form of communication in our current society, but at the same time … provide some degree of quality control, given the risks that many forms of electronic communication can be manipulated" (*Donaldson*, at para. 4).

Means of Establishing Integrity

[94] Sections 31.2-31.5 of the *Act* address how the best evidence rule in respect of an electronic document is satisfied by either proof of the integrity of the electronic documents system or if an evidentiary presumption of integrity applies. *The Law of Evidence* explains the four statutory means of meeting this requirement at 564-565 as follows:

> "In the *Canada Evidence Act*, there are four alternative ways to satisfy the 'best evidence' requirement for admission, and according to section 31.6, each of these alternatives can be demonstrated with affidavit evidence:
>
> 1) Under section 31.2, by proving, on the balance of probabilities, the 'integrity of the electronic document system' – in other words, that the computer that generated or stored the document was working properly. This can be done directly through evidence of a witness familiar with the creation of the document who recognizes that the document retrieved from the computer is accurate. This can also be done circumstantially, under section 31.5, by showing that the electronic document system operated according to the relevant standards, procedures, usages, and practices in the relevant business, endeavor, or enterprise.
>
> 2) Under section 31.3, by relying on a statutory presumption of 'the integrity of the electronic document system' – namely:
>
> - Under section 31.3(a), the 'functioning system' presumption, triggered by evidence 'capable of supporting' a finding that, at all material times, the computer system was operating properly, or, if not, that the improper functioning did not affect the integrity of the document. The kind of evidence produced in *R. v. Woodward* [1]– that numerous messages were successfully sent and received using the system – should suffice. This presumption can be rebutted by evidence to the contrary.
> - Under section 31.3(b), the 'party adverse in interest' presumption, which presumes the integrity of a document proved to have been recorded or stored by a party adverse in interest to the party seeking to introduce it. As the source of the document, the party adverse in interest is in a position to challenge its integrity and therefore bears the onus of doing so. This presumption is useful for documents received in disclosure from the

[1] *R. v. Woodward*, 2011 ONCA 610

opposing party during litigation, documents obtained during the execution of a search warrant from a computer possessed by the accused[2], or documents that can be linked by evidence to the computer account of the opposing party litigant[3].

- Under section 31.3(c), the non-party business record presumption, triggered by proof that the electronic document was recorded or stored by a non-party, independently of the parties, in the usual course of business.

3) Under the combined effect of sections 31.2(1) and 31.4, through proof of an electronic signature by a person identified by the electronic signature.

4) Under section 31.2(2), by relying on the statutory presumption that the information on a printed electronic document has been manifestly or consistently relied on or used. This rebuttable presumption operates on the inference that a document that has been manifestly or consistently relied upon must be believed by its customary use to be reliable."

Standard of Proof for Integrity

[95] As I stated previously, the standard of proof of integrity of electronic records differs depending upon where reliance is placed.

[96] If reliance is placed upon section 31.3(a) the standard is, once again, modest as the wording mirrors that of section 31.1 ("some evidence capable of supporting") (*Proof and Progress,* at 204).

[97] If reliance is placed upon either 31.2(1)(a) or (b), 31.3(b) or 31.3(c), which sections require either "proof" or that it is "established", I agree that the standard is on the balance of probabilities (*Proof and Progress*, at 202 and 207-210).

Establishing Integrity in this Instance

[98] On the facts of this case I agree that the only potential means of establishing integrity was under section 31.3(a) (the "functioning system" presumption).

[99] The majority concludes that this is satisfied by the testimony of the police officers. Respectfully, I disagree.

---

[2] *R. v. Avanes*, 2015 ONCJ 606, at para. 63
[3] *R. v. Hirsch*, 2017 SKCA 14, at paras. 23-29

[100] Section 31.3 references "the integrity of an electronic documents system by or in which an electronic document is recorded or stored". Interpreting this phrase (or the phrase within subsection 31.3(a)) "the computer system or other similar device used by the electronic documents system was operating properly" with focus on the computer system at the police station would be inconsistent with what I have accepted as the purpose of the proof of integrity/best evidence provisions of the *Act*.

[101] The officers' testimony that the screenshots the police printed were the same as they received on their system could not, in my view, entitle the Crown to rely on the "functioning system" presumption in section 31.3(a). It could not provide for the screenshots some "degree of quality control, given the risks that many forms of electronic communication can be manipulated" (*Donaldson*, at para. 4). It could not provide any assurance that the screenshots downloaded from their system were the same as had allegedly been posted by Mr. Martin, viewed by an unidentified third party and forwarded to the police (*The Law of Evidence*, at 564). Testimony from the person whose system purportedly "recorded and stored" the screenshots allegedly posted by Mr. Martin or from a person who retrieved the screenshots from an electronic device used by Mr. Martin would be needed to establish system integrity in this instance.

[102] If all that was required to benefit from the presumption of system integrity stated in section 31.3(a) was a functioning computer system at the police station, in my view there would be no need for the *Act* to provide alternative means of establishing integrity. A record of any kind, forwarded to the police from an unidentified source and printed from their system, would meet the integrity requirements for admissibility.

[103] I accept instead the interpretation applied in *R. v. Bernard*, 2016 NSSC 358.

[104] In *Bernard* the accused was charged with second degree murder and the Crown sought to rely on photographs of the accused's Facebook wall which they alleged helped to show that the accused intended to commit the crime. Proof of integrity was found to be lacking for the photographs because they were taken by a third party and forwarded to a witness who testified but could not recall their source. The Court highlighted the difference between a photograph of a Facebook conversation between two users and a photograph of a post to a user's Facebook wall (paras. 54-55) and concluded that system integrity could not be established in the absence of evidence of the origin of the screenshots or access by the Crown to the Facebook account directly (paras. 56-57).

[105] I also disagree that it can be inferred from Constable Walsh's evidence that the screenshots had not been altered. Respectfully, there was nothing in Constable Walsh's testimony that would permit such an inference. Because the source was anonymous, the officer was unable to identify the system that had "recorded or stored" the screenshots. Without identification of the system, the officer could offer nothing to assist in determining whether that system was working properly.

[106] I conclude that even on the modest threshold which applies to subsection 31.3(a), the "functioning system" presumption of integrity could not be relied upon in this case because:

- the system that had recorded or stored the screenshot was never identified and there was no evidence that it was working properly;
- the person who purportedly saw the Facebook posting and sent it to the police did not testify (or provide an affidavit as permitted under section 31.6);
- no computer or cell phone was located during the execution of the search warrant at Mr. Martin's home; and
- the police (who sought to enter the evidence) had conducted an electronic search and had not been able to access a Facebook page for Mr. Martin.

[107] All that the police officers could say was that their own system (which had received a copy of the screenshots from the anonymous complainant) was working properly and that the printed copies of the screenshots from their system were the same as those received from the anonymous source. I adopt the reasoning in *Bernard*, at paras. 52 and 56-57 and *Donaldson*, at paras. 12-17 and conclude that this testimony is insufficient to establish integrity. It could not address the risk that the screenshot could have been manipulated before its receipt by the police. There was no evidence that what was input, was what was output.

Jurisprudence on the Integrity Provisions

[108] With respect to jurisprudence that specifically addressed section 31.3(a), I note that in *S.H.*, the data was extracted by the police from a third party cell phone. Section 31.3(a) was satisfied because the police had the phone and were able extract the data. A qualified officer testified that a disc copy of the data accurately reflected data downloaded from the phone which reflected

conversations that were "contextually consistent with other facts in (the) case" (para. 27).

[109] In *Richardson* the MSN messages were originally saved and stored on a computer of a witness who testified on the *voir dire* about the conversations he had with the accused. The conversations had been seen on a third party's computer by another witness who found them inappropriate, emailed them to herself and gave them to a mentor at church (para. 38) who provided them to the police. There was evidence that the electronic documents transmitted were accurate displays of the data originally input into the relevant computer because the witnesses testified respectively as to what they remembered seeing on the third party's computer, and/or what they sent, received or printed. On this basis the New Brunswick Court of Appeal agreed that the trial judge had correctly concluded that integrity was established (at paras. 45-46).

[110] In *Ball* the Facebook messages that the witness had received and brought up on a police station computer were entered by the Crown at trial without consideration of either the statutory framework or the distinct evidentiary nature of the content of the messages (para. 82). However, the court considered that it was "neither necessary nor desirable … to determine, at the first instance, whether the photographed Facebook messages met the statutory best evidence rule on a balance of probabilities". The ratio of the decision with respect to system integrity is that "the judge should have made [this] determination in the first instance, on a *voir dire*, in the absence of the jury" (para. 87). This error (and others) caused the court to conclude that a new trial should be ordered (paras. 121-122).

[111] In *Durocher* the complainant testified that she had received the Facebook messages from the accused by email on her Smartphone and her testimony was unchallenged (paragraph 95). This evidence supported integrity of the system.

[112] In *Donaldson,* the electronic documents had been sent to the complainants from a Facebook account attributed to a third party. Justice Paciocco stressed the importance and purpose of the *Act*'s provisions and explained their operation (paras. 4-10).

[113] With specific reference to integrity, Justice Paciocco explained that there were presumptions "relating to when documents are sufficiently quality-controlled to gain admissibility" but that in order to satisfy either presumption for proof of integrity, the Crown required "questioning of witnesses to show the nature of the electronic document system that was utilized to secure the

message, and evidence about the historical successful use of that system" (para. 9).

[114] Specifically, with respect to the "functioning system" presumption in section 31.3(a), while the Court held at paragraph 10 that proof that "the system on which the documents were received was functioning properly "triggers a presumption", this statement must be read in the context of paragraph 9, which I have cited above. Applied to the facts of the within case, functioning of the system at the police station could not provide sufficient quality control for admissibility. I would not interpret *Donaldson* to suggest that, on the facts of this case, the "electronic documents system" under consideration was that at the police station. In my view it is the system used by the unidentified source or, as stated previously, the system purportedly used by Mr. Martin.

[115] Consistent with this interpretation, in *Soh*, system integrity was supported by the complainant's testimony concerning messages she had exchanged with the accused. This testimony confirmed that the system used to record the Facebook images and messages was functioning properly.

[116] Finally, in *J.V.*, the Crown sought the admission of documents in the form of electronic records of a Google Hangout conversation between the complainant and the accused. Two formats of the conversation were presented. The first was a series of photographs that depicted the conversation displayed on a cellphone. The second was an Excel spreadsheet created using software to download the contents of a Google Hangout account that was used by an expert witness. Although referenced as "screen photographs", I note that the images did not capture an event, but merely a conversation. Both formats of the documents were admitted. With respect to section 31.3(a), Justice Paciocco found that the complainant's testimony (that the evidence depicted a conversation she had) was circumstantial evidence that satisfied the presumption.

[117] The testimony received in each of these authorities, relative to the electronic system in question, is absent in this case.

Other Common Law and/or Statutory Rules

Section 31.7

[118] The necessity for "parties to consider the electronic evidence provisions alongside more established rules" arises from the wording of section 31.7 (which I have cited in full at para. 87) and is discussed in *The Law of Evidence*

in Canada, at 1351-1356. Referencing *Saturley v. C.I.B.C. Worldmarkets Inc.*, 2012 NSSC 226, at paras. 11-13, the authors state:

> "18.97
>
> On the *Saturley* approach, an analysis is conducted to determine whether additional evidential considerations must be applied beyond the statutory requirements governing electronic information. Justice Wood explained:
>
> > It is possible that a given item of electronic information may have aspects of both real and documentary evidence. For example, an email in electronic form will include electronic data identifying the computer on which it was created and when it was sent. That information is added automatically by the computer software and would likely constitute real evidence. If the content of the e-mail is being introduced for its truth, it would be considered a document and subject to admissibility as such.
>
> 18.98
>
> This analysis appears to accord with s. 31.7 of the *Canada Evidence Act*, which states that ss. 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. The ongoing applicability of hearsay and documentary evidence rules to electronic information makes sense. …"

[119] This approach was endorsed in *Ball*, at para. 68. It was applied in *Soh*, at paras. 32-52; *J.V.*, at paras. 3 and 31-32; *Durocher*, at paras. 68-73; and *S.H*, at para. 10, where, in each case, the additional evidential considerations related to hearsay. The same approach was also recently applied by this Court in *Jennings* which decision confirms the factors to be considered on the admissibility of photographs as part of the courts' gatekeeper role to assessment of probative value/prejudicial effect. (In *Jennings* it was relative to audio-visual recordings obtained from a doorbell recording system (paras. 14 and 17)).

Photographic Evidence

[120] When a photograph or video "is admitted simply to identify someone", what is being authenticated is the image and not the event depicted. In comparison, "[p]hotographs that purport to depict an event are apt to require more" (*The Law of Evidence*, at 560).

[121] The Crown sought to rely on the events depicted in the screenshots. In my view, this required application of the common law considerations for threshold admissibility of photographic reproductions.

[122] This Court in *R. v. Penney,* 2002 NFCA 15 recognized the trend "toward a less stringent test for the admissibility of evidence generally" (para. 10) but held that "a broadly based general principle of inclusion does not relieve the Court of its responsibility to scrutinize the evidence" (para. 12). As an exercise of the judge's gatekeeper function, this Court applied the three-part test from *Creemer* to the assessment of the probative value of a videotape and acknowledged that its admissibility required the proponent to establish:

(1) its accuracy in truly representing the facts;

(2) its fairness and absence of any intention to mislead; and

(3) its verification under oath by a person capable of doing so.

Burden of Proof on the Creemer Test

[123] Cameron J.A. in concurring reasons in *Penney* suggested that the standard of proof for the exercise of the gatekeeper function for photographic evidence was on a balance of probabilities (at para. 49). This conclusion is consistent with the language used in the *Creemer* test ("establish") which is, as I have previously stated, the language used in those sections of the *Act* where a balance of probabilities standard of proof applies (see para. 97). This differs from the standard of proof for authenticity under section 31.1 and integrity under subsection 31.3(a) of the *Act.*

[124] It follows that the *Creemer* test is not embedded in the statutory test for authenticity in section 31.1; more is required when the Crown seeks to rely upon the events depicted in the images.

Application of the Creemer Test to the Facts

[125] In my view, the *Creemer* considerations for assessing accuracy of the representation could not be met on the facts of this case. While "the person verifying the authenticity of the photographic or video tapes need not be the photographer", it must be someone who can speak to their accuracy and testify, "that those photographs or videotapes are fair and accurate reproductions of what" the witness observed (*The Law of Evidence,* at 559).

[126] There was no witness who had observed either Mr. Martin's Facebook page or what was depicted on the screenshots; the police had never seen him hold a weapon.

[127] Without verification under oath by a person capable of doing so, neither the accuracy of the photographs in truly representing the facts nor their fairness and absence of intent to mislead could be established. I conclude that the *Creemer* test for threshold admissibility of photographic evidence was not satisfied.

CONCLUSION

[128] The Judge conducted a *voir dire* following which she gave an oral decision in which she referenced *Soh* and *Hirsch.* Her decision predated *Ball, Durocher, S.H., C.B.,* and *Richardson* so she did not have the benefit of this helpful jurisprudence. In assessing threshold admissibility, she relied upon the common law *Creemer* test for photographic evidence but not sections 31.1 - 31.8 of the *Act* in addition.

[129] The Judge referenced the testimony of the police officers and the findings of fact that could be drawn from it. While there was an error made in the recognition and application of the law respecting threshold admissibility of electronic documents, for the reasons stated herein, I find her conclusion (that the evidence was inadmissible) to be correct.

[130] For these reasons I would therefore have dismissed the appeal.

_____

G. D. Butler J.A.