THE CANADIAN BAR ASSOCIATION

EFFECTIVELY FINDING AND USING SOCIAL MEDIA EVIDENCE IN LITIGATION

THE ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE
MAY 12, 2022

JUDGE WAYNE GORMAN
THE PROVINCIAL COURT OF NEWFOUNDLAND AND LABRADOR

INDEX

Introduction:

In this paper I intend to review the law as regards the admissibility of what has been described in Canada as "social media evidence", i.e. text messages, Facebook postings, selfies, etc. (see Lisa A. Silver, *The Unclear Picture of Social Media Evidenc*e, (2020) 43-3 Manitoba Law Journal 111, at page 111). Professor Silver has noted that "social media is often the context in which criminal offences can be committed. It can provide a space in which offences are committed and it can provide proof of it as well" (at pages 117 to 118).

A useful manner in which to describe social media evidence is to adopt the approach of the *Canada Evidence Act*, R.S.C. 1985, which uses the phrase an "electronic document" (see section 31.8).

It has been pointed out that "[e]lectronic evidence poses unique problems from an evidentiary standpoint. One problem is classification. Are records generated on, or even by, a computer analogous to documents, to real evidence, or to neither? Is a printout the original? Are there any 'originals' for electronic evidence?" (see Casey Hill, David M. Tanovich and Louis P. Strezos, *McWilliams' Canadian Criminal Evidence* (5th. ed., Toronto: Canada Law Book, loose-leaf, at paragraph 24:90.10).

It is important to understand that social media evidence must be admissible based upon its form and its use. It is not automatically admissible. It must be relevant to a point in issue and not excluded by a rule of evidence (such as the general prohibition on leading evidence of a previous consistent statement, etc.). Having said this, social media evidence can constitute reliable, compelling and significant evidence that can at times be difficult to refute.

This paper will concentrate on the admissibility of social media evidence in criminal matters. I will consider the admissibility of social media evidence in Canada at common law and its admissibility pursuant to the *Canada Evidence Act*. This latter analysis may have some crossover to admissibility in civil matters, but the jurisprudence analyzed will be primarily of a criminal nature. First, however, a few comments on the necessity of conducting a *voir dire* and authentication.

Does a Trial Judge Have to Hold a *Voir Dire* When Social Media Evidence is Sought to be Introduced?

In ***R. v. Durocher***, 2019 SKCA 97, this question arose in the context of a sexual assault trial in which the Crown was allowed to introduce text messages said to have been sent by the accused to the complainant (L.A.) through Facebook. The Crown sought to have the messages considered as an admission made by the accused to

someone who was not in a position of authority and thus admissible without a *voir dire* being conducted (see ***R. v. S.G.T.***, 2010 SCC 20, at paragraph 20).

L.A. testified that the accused "had sent Facebook messages to her several days before the alleged assaults took place". When L.A. was asked how she knew that it was the accused who had sent her the messages, she responded: "Because it says his name" (at paragraphs 8 and 29).

These messages were entered as evidence without a *voir dire* being held. The accused was convicted and appealed, arguing that the trial judge erred in allowing the social media evidence to be introduced without conducting a *voir dire*.

The Saskatchewan Court of Appeal:

The Saskatchewan Court of Appeal held that a *voir dire* was not necessary "to address threshold admissibility when authorship is in issue. Considering that the authorship of the Facebook messages was at issue, the trial judge was only required to consider whether the evidence proved on a balance of probabilities that Mr. Durocher wrote the Facebook messages" (at paragraph 46). The Court of Appeal stressed that in "exercising his gatekeeper function at the threshold admissibility stage, the trial judge only needed to be satisfied on a balance of probabilities that the statements were made by Mr. Durocher. He was entitled to rely on circumstantial evidence to do so and, importantly, he was not required to hold a *voir dire* to make a threshold determination at this stage" (at paragraph 52).

This, however, appears to "beg the question". Authentication will always require some evidence. How is this evidence to be considered without a *voir dire* if the admissibility of the evidence is contested? This does not mean that the *voir dire* has to be extensive. But, if it is argued that the statement was not made by the accused, some evidence that it was must be presented. As noted in ***R. v. Ball***, 2019 BCCA 32, "as with other admissibility issues, where there is reason to question whether an electronic document meets the statutory requirements, a *voir dire* should be held and a reasoned determination made as to its admissibility" (at paragraph 67).

R. v. Ball:

In ***Ball***, the accused was convicted of the offence of arson. At his trial, his girlfriend (Ms. Lacey) testified that the accused had sent her Facebook messages indicating that he had committed the offence. The Crown introduced photographs the police had taken from a computer screen illustrating the contents of the messages. The British Columbia Court of Appeal noted that Ms. Lacey "was the only Crown witness called to explain the operation of Facebook Messenger, which she

characterized as similar to text messaging". A *voir dire* had not been held to determine admissibility.

The accused appealed from conviction. The appeal was allowed and a new trial was ordered. The British Columbia Court of Appeal pointed out that the Facebook messages "were extremely important Crown evidence. They included Mr. Ball's alleged admission to setting the fires and a computer-generated time stamp associating the first message with the time" of the fire....Nevertheless, their admissibility was not questioned and a *voir dire* was not conducted. Therefore, the judge did not make a reasoned determination on whether the photographed messages were admissible and, if so, the permissible use for their computer by-product content" (at paragraph 81).

Proof of Authentication on the Voir Dire:

Professor Silver notes that authenticity "requires an investigation into whether the real evidence is what it claims to be. This differs from testimonial evidence where the person, for admissibility purposes, is taken at their word, leaving credibility issues for the final determination" (*The Unclear Picture of Social Media Evidenc*e, at page 122). She concludes that "an electronic evidence admissibility *voir dire* should be required in all instances where social media evidence will be introduced. This is so 'a reasoned determination' may be made on its admissibility. The trial judge should not wait for counsel to engage the process but should raise the issue at the outset. For consistency, the *voir dire* should apply the admissibility regime under the *Canada Evidence Act*" (at page 153).

Interestingly, in ***Durocher***, despite having concluded that the trial judge did not err in failing to hold a *voir dire*, the Court of Appeal indicated that that it would have been "preferable" for a *voir dire* to have been held in relation to whether the *Canada Evidence Act's* threshold authenticity and integrity requirements had been established by the Crown (at paragraph 96):

> Since the Crown sought to adduce electronic documents into evidence, it would have been preferable for the trial judge to have conducted a *voir dire* to determine threshold authenticity and integrity. However, bearing in mind the low bar attached to s. 31.1, the functional approach adopted by the courts with regard to its application, the presumption of integrity under the *CEA* and the fact the trial judge ultimately found Mr. Durocher was the author of the Facebook messages, I am satisfied that the evidence adduced by the Crown was capable of authenticating the Facebook messages.

One final comment before leaving ***Durocher***. ***Durocher*** is a good illustration of the dual evidentiary nature of social media evidence. To be admissible, such evidence must comply with the threshold requirement set out in section 31.1 of the *Canada Evidence Act*, but it must also be otherwise admissible. In ***Durocher***, this latter requirement was met by the Crown seeking to use the Facebook message as an admission. Though a *voir dire* was not required for the latter, it was required for the former.

A Summary:

In summary, despite what may have been said in ***Durocher***, I would suggest that anytime an objection to the introduction of social media evidence is raised, it is imperative that a *voir dire* be conducted. Counsel should be able to advise the presiding judge of the purpose of the proposed evidence and the electronic nature of that evidence. There may be times that admissibility can be readily established, but this does not alter the *voir dire* requirement.

Finally, if you are seeking to introduce social media evidence and the consent of the opposing party has not been obtained, you should be in a position to establish any admissibility criteria that applies. For social media evidence, this can include being able to verify the origin of the item, its authenticity and its reliability, both at the time of creation and at the time admission is sought.

As will be seen, these latter issues may be considered as going to weight rather than admissibility, but they can be crucial to the evidence being impactful. Any social media evidence a party seeks to have admitted must be presented to the court in some form that can be considered and if necessary, entered as an exhibit. You should never, for instance, find yourself in the position of having a copy of an electronic message that you are seeking to have admitted without being able to establish such elements as origin, reliability and continuity (see ***R. v. Wolfe***, 2022 SKQB 86, at paragraphs 14 to 16).

As a result, the following types of questions may require answers, but certainly require your consideration:

-Where is the “original” electronic document held (is there such a thing?);

-Is that device available;

-Is the electronic document still on that device (see ***R.G. v. J.G.***, 2022 ONSC 1678, at paragraph 181);

-Can you prove who sent the electronic document or who received it;

-Why is the electronic document relevant;

-Does its admission offend any exclusionary rule;

-If you are seeking to introduce a screen shot or a photocopy of the electronic document, who made the copy or took the screen shot; and

-Is there a witness who can testify that the electronic document or the copy of it has not having been altered?

The point to keep in mind is that electronic documents are subject to specific and general rules of evidence. What I mean by this is that the *Canada Evidence Act* contains provisions which specifically govern the admissibility of electronic documents. These provisions apply to social media evidence. However, such evidence is also subject to the general rules of evidence, including relevance and exclusionary rules.

As a result, it is not sufficient to establish that the social media evidence meets the test for admissibility set out by the common law or the Canada Evidence Act (by having been authenticated), it must also be established that the document's admissibility conforms with the law of evidence that applies based upon nature, content, and purpose for which the social media evidence is being introduced.

Accordingly, if it is being used as a confession, for instance, the requirement for proof of voluntariness applies. If it constitutes a prior consistent statement or hearsay, then the general prohibition against the admission of such evidence is applicable. In other words, social media evidence will always have two components that go to admissibility: the electronic nature of the document and the purpose for which it is sought to be introduced. In relation to the former, admissibility is premised upon authentication.

Authenticating Electronic Evidence:

Evidence in the form of text messages, Facebook postings and other forms of electronic communication are now common forms of evidence sought to be introduced in Canadian courts. Such evidence can be used for various purposes, including as a prior inconsistent statement and as narrative (see ***R. v. Vigon-Campuzano***, 2022 ONCA 234). Such evidence can be of great probative value, though it can raise concerns about how reliability can be ensured. Therefore, the admission of such evidence, like many forms of evidence, requires proof of authentication, including in certain cases for instance, proof that the electronic document was sent by a relevant party.

Having said this, the admissibility of the contents of text messages or electronic documents is similar to the admissibility of other forms of communications or documents. It is not the content of the evidence that is new, it is the format that is

new. For instance, there would be nothing wrong with counsel cross-examining a witness on a telephone call purportedly made to the accused or for the Crown seeking to introduce a letter sent to by the accused to the complainant, if relevant. This is, subject to authentication, no different than using a Facebook posting for the same purpose.

The authors of *Electronic Evidence in Canada* (Graham Underwood and Jonathan Penner, Thomsen Reuters, loose-leaf) point out that "proof of authenticity and reliability is not concerned specifically with the substantive content of the proffered ESI [electronically stored information], but rather with where the ESI comes from, how it was obtained and handled, whether it can be trusted to be what it purports to be, and how reliable a source of information it is about a material issue" (at page 11-11).

The authors also point out that authenticity "is not the same as reliability. 'Authenticity' refers to the quality of the ESI in being what its proponent claims it to be. Authenticity is a measure of the likelihood that the proffered ESI is actually what it is described as, whereas 'reliability' is a measure of how well the proffered ESI communicates useful information about a matter that is in dispute" (at page 11-15).

The Court of Appeal of Newfoundland and Labrador has made the same point, holding that "authentication does not mean the document is genuine...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" (see ***R. v. Martin***, 2021 NLCA 1, at paragraph 49).

The Two Stages of Authentication:

Authentication has two distinct stages: threshold admissibility and ultimate weight. It has also been held that the "threshold for authentication of evidence, both at common law and under s. 31.1 of the *Canada 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'" (see ***R. v. Farouk***, 2019 ONCA 662, at paragraph 60). I intend to consider the admissibility issue from both the common law perspective and how this is achieved through the *Canada Evidence Act*.

A**uthentication at Common Law:**

In ***Durocher***, it was noted that at "common law, authentication is a prerequisite to the admissibility of a document at trial". The Saskatchewan Court of Appeal

explained that "this 'simply means that the trier of fact must be satisfied that the document in issue is what it purports to be'…Methods of authentication include *viva voce* testimony, common law rules and presumptions, or statutory instruments" (at paragraph 75).

The issue of authentication was also considered by the Ontario Court of Appeal in ***R. v. C.B.***, 2019 ONCA 380. This case illustrates how easily authentication can be established. In ***C.B.***, the accused was convicted of the offence of sexual assault. At his trial, the complainant (DP) was cross-examined on text messages she had purportedly exchanged with the accused. This was designed to contradict her testimony. DP agreed that the telephone number from which the text messages were sent was her cellphone number.

In convicting the accused, the trial judge held that the questioning of the complainant in relation to the text messages was of no "probative value" because it had not been established that DP had sent the messages. On appeal, the Ontario Court of Appeal ordered a new trial, holding that the trial judge "erred in concluding that the text messages had no probative value because they had not been properly authenticated by direct evidence" (at paragraph 73).

The Ontario Court of Appeal:

The Ontario Court of Appeal indicated that "the requirement of authentication applies to various kinds of real evidence. Authentication involves a showing by the proponent of the evidence that the thing or item proffered really is what its proponent claims it to be…At common law, authentication requires the introduction of some evidence that the item is what it purports to be. The requirement is not onerous and may be established by either or both direct and circumstantial evidence" (at paragraphs 64 and 66).

The Court of Appeal pointed out that "text messages may be linked to particular phones by examining the recorded number of the sender and receiving evidence linking that number to a specific individual, as for example, by admission…As a matter of principle, it seems reasonable to infer that the sender has authored a message sent from his or her phone number. This inference is available and should be drawn in the absence of evidence that gives an air of reality to a claim that this may not be so. Rank speculation is not sufficient…And even if there were an air of reality to such a claim, the low threshold for authentication, whether at common law or under s. 31.1 of the *CEA*, would seem to assign such a prospect to an assessment of weight" (at paragraphs 70 and 72).

The Ontario Court of Appeal concluded that the evidence presented at the trial was "capable of supporting a finding that the text messages were what they purported to

be: an exchange of communications between D.P. and the appellant C.B. The trial judge erred in holding, as he appears to have done, that the authenticity threshold could only be met by direct evidence from the sender or expert opinion evidence from a forensic examiner" (at paragraph 77).

Thus, the simple admission that the text messages came from the witness' telephone was a sufficient basis for authentication and therefore admissibility.

As noted earlier, in ***Durocher***, the issue involved text messages said to have been sent by the accused to the complainant (L.A.) through Facebook. The accused was convicted at trial and appealed from conviction, arguing that the trial judge erred in allowing this evidence to be introduced. The accused argued that it had not been proven that he sent the text messages.

On the issue of admissibility, the Saskatchewan Court of Appeal held that for "purposes of threshold admissibility, the Crown had to establish there was some evidence capable of supporting a finding – on a balance of probabilities – that the Facebook statements were made by Mr. Durocher" (at paragraph 48).

In considering this question, the Court of Appeal referred to the Supreme Court of Canada's decision in ***R. v. Evans***, [1993] 3 S.C.R. 653, in which the Supreme Court indicated that when the authorship of a statement attributed to an accused is in issue, a two-staged approach should be adopted (at page 668):

> …the matter must be considered in two stages. First, a preliminary determination must be made as to whether, on the basis of evidence admissible against the accused, the Crown has established on a balance of probabilities that the statement is that of the accused. If this threshold is met, the trier of fact should then consider the contents of the statement along with other evidence to determine the issue of innocence or guilt. In the second stage the contents are evidence of the truth of the assertions contained therein.

The Court of Appeal concluded in ***Durocher*** that the trial judge "properly applied the ***Evans*** test to determine threshold admissibility. Examining the circumstantial evidence as a whole, it was open to him to draw an inference that Mr. Durocher was the author of the Facebook messages. L.A. provided *viva voce* testimony and a statement to the police that Mr. Durocher was the person who had sent the Facebook messages to her" (at paragraph 50).

The Court of Appeal stressed that in "exercising his gatekeeper function at the threshold admissibility stage, the trial judge only needed to be satisfied on a balance of probabilities that the statements were made by Mr. Durocher. He was entitled to rely on circumstantial evidence to do so" (at paragraph 52).

In summary, the test for authentication and thus admissibility of social media evidence in Canada, at common law, involves a very low threshold which can easily be established. What if the party seeks admission of an "electronic document" pursuant to the provisions of the *Canada Evidence Act*?

The Canada Evidence Act:

The issue of authentication of social media evidence has been addressed by Canadian judges through both the common law and the *Canada Evidence Act*. In ***R. v. Hirsh***, 2017 SKCA 14, it was suggested that the provisions in the *Canada Evidence Act* dealing with the admissibility of social media evidence "is a codification of the common law rule of evidence authentication" (at paragraph 18). This is true, but as will be seen, the statutory provisions are much broader than that, including how an "electronic document" is defined.

What is an Electronic Document?

The *Canada Evidence Act* contains a number of provisions dealing with the admissibility of "electronic documents". Section 31.8 provides the following broad definition of what constitutes an "electronic document":

> "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.

This definition has been described by one author as "a definition of imposing breadth, particularly when combined with the definition of 'data' in subsection 31.8—'representations of information or of concepts, in any form.' The statutory provisions do not therefore catch only documents in the conventional sense. They also catch at least some audio and video recordings" (see David M. Paciocco, *Proof and Progress: Coping with the Law of Evidence in a Technological Age*, (2013) 11 Can. J. L. & Tech. 181, at page 190).

Justice Paciocco also suggests that this "definition is broad enough to cover copies of all documents stored in a computer, such as business records, bulletin boards from Facebook or other social media, emails and or 'tweets'" (at page 189).

A Computer System:

The *Canada Evidence Act* also defines what constitutes a "computer system". Section 31.8 provides the following definition:

> computer system means a device that, or a group of interconnected or related devices one or more of which,
>
> (a) contains computer programs or other data; and
>
> (b) pursuant to computer programs, performs logic and control, and may perform any other function.

In ***R. v. Richardson***, 2020 NBCA 35, the New Brunswick Court of Appeal held that that "[f]acebook posts and messages, e-mails and other forms of electronic communication fall within the definition of an 'electronic document.' Home computers, smartphones and other computing devices fall within the definition of a 'computer system'…Likewise, MSN messages recorded or stored on a computer are 'data' which falls within the definition of an 'electronic document', as well as any "display, printout or other output of that data" (at paragraph 22).

In ***R. v. Ball***, 2019 BCCA 32, the British Columbia Court of Appeal considered the definitions of "electronic document" and "computer system" in the *Canada Evidence Act*. The Court of Appeal indicated that "Facebook posts and messages, emails and other forms of electronic communication fall within the definition of an 'electronic document'. Home computers, smartphones and other computing devices fall within the definition of a 'computer system'. Accordingly, the admissibility of Facebook messages and other electronic communications recorded or stored in a computing device is governed by the statutory framework" (at paragraph 67).

The broad definitions provided ensures that all forms of social media evidence will be subject to the admissibility criteria set out in the *Canada Evidence Act*, which is set at a minimal level.

What is the test for admissibility?

Admissibility Pursuant to the Canada Evidence Act:

Section 31.1 of the *Canada Evidence Act* sets out the test for admissibility of "electronic documents".

Under the heading, "Authentication of electronic documents", section 31.1 reads as follows:

> 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.
>
> [My emphasis]

This is the same test applied at common law and as we saw earlier, it creates a very low threshold for admissibility. If, for instance, a witness says: "I received or sent this text message from or to Mr. Smith", then subject to relevance, the text appears to be admissible. In ***Hirsch***, it was noted that section 31.1 of the *Canada Evidence Act* "merely requires the party seeking to adduce an electronic document into evidence to prove that the electronic document is what it purports to be. This may be done through direct or circumstantial evidence" (at paragraph 18).

What Does the Phrase "the electronic document is that which it is purported to be" mean?

It does not appear that this means anything beyond identifying the item sought to be introduced. Is it a Facebook posting, an e-mail? In addition, this appears to be easy to establish. In ***Durocher***, for instance, the issue was proof that the documents received by the complainant from the accused were a Facebook text messages. The Court of Appeal concluded this had been established because the witness who received the messages "provided some evidence capable of supporting a conclusion that [the messages were] what [she] claimed it to be" (at paragraph 94).

What was that evidence? The witness testified that accused sent her the text messages.

Capable of Supporting a Finding:

In ***Martin***, the Court of Appeal for Newfoundland and Labrador pointed out that section 31.1, by stipulating that there must be evidence "capable of supporting a finding" that the electronic evidence sought to be admitted is what it purports to be, creates a very low threshold for admissibility". The Court of Appeal held that "[e]vidence '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…section 31.1 does not limit how or by what means the threshold may be met…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" (at paragraph 47).

However, another Canadian Court of Appeal has expressed a note of caution. In ***R. v. Aslami***, 2021 ONCA 249, the accused was convicted of an offence in which the primary evidence against him was phone and Facebook messages he purportedly sent to his former partner. In setting aside the conviction, the Ontario Court of Appeal noted that the cell phone number from which the messages were sent was registered to someone other than the accused. The Court of Appeal cautioned trial judges to "be very careful in how they deal with electronic evidence of this type. There are entirely too many ways for an individual, who is of a mind to do so, to make electronic evidence appear to be something other than what it is. Trial judges need to be rigorous in their evaluation of such evidence, when it is presented, both in terms of its reliability and its probative value" (at paragraph 30).

In addition, the nature of social media postings has to be recognized. Not everything posted on Facebook, for instance, is posted with an intention of accuracy or solemnity. This issue arose in the case of ***R. v. Robinson***, [2021] NICA 65, in which the accused was convicted of the murder of a prison official (Mr. Ismay) by attaching an explosive device to his car while it was parked outside his home. Part of the evidence against the accused included his Facebook postings in which he expressed support for what the Court of Appeal of Northern Ireland described as "violent Irish Republicanism" (at paragraph 42). On appeal, the accused argued that the trial judge had placed too much weight on these postings.

The Court of Appeal agreed that it would be an error to read "too much into the Facebook images" (at paragraph 66). However, the Court of Appeal upheld the conviction, concluding that though "the learned trial judge may have placed a little too much emphasis on the appellant's Facebook pictures and his political support…this does not affect the overall result in this case given the overwhelming amount of other evidence about the appellant's motivations and interests in the run up to Mr. Ismay's murder" (at paragraph 68).

Caution as regards the integrity of electronic communications may be of value, but it is important not to confuse weight and admissibility. It is clear that the threshold for the admissibility of electronic documents is a very low one. The problem in ***Alsami*** was not the potential for manipulation (see ***R. v. GS***, 2022 MBCA 35), but

the fact that the messages had been sent from someone else's phone.[1] If it had been established that the messages had been sent from a phone owned by the accused, then the evidence would appear to have been admissible and any concerns of manipulation would have to be addressed when the weight of the messages was assessed. In addition, the "presumption of integrity", created by the *Canada Evidence Act* for electronic documents, must be considered.

The "Best Evidence Rule" and a Presumption of Integrity:

Sections 31.2(a) and (b), of the *Canada Evidence Act* indicate that 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]

Section 31.3 creates a "presumption of integrity" in relation to electronic documents by deeming such documents to be reliable and accurate, "in the "absence of evidence to the contrary":

> For the purposes of section 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic document 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;

---

[1] Also see ***R. v. Kerr***, 2022 SKPC 2, at paragraphs 35 to 37, and ***R. v. Hermkens***, 2021 ABQB 1016, at paragraph 67.

[2] Section 31.4 of the *Canada Evidence Act* states as follows:

> *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.*

> (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.

It has been suggested that "the purpose" of these provisions "is to provide a shortcut for authentication by focusing on the reliability of the electronic documents system rather than on the evidence itself" (see David M. Tanovich, *R. v. Andalib-Goortani: Authentication & The Internet* (2014), 13 C.R. (7th) 140, at page 142).

If one of the above prerequisites is established, document integrity is deemed to exist, unless the opposing party presents "evidence to the contrary", which is capable of rebutting the presumption (see section 31.3).

The Manner of Usage:

The matters referred to in sections 31.2(2) and 31.3, can be established by affidavits (see section 31.6(1)). In addition, the *Canada Evidence Act* provides further assistance to the party seeking admission of an electronic document by allowing evidence of the manner of "usage" of the system from which the electronic document was retrieved. Section 31.5 states:

> 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.

Based upon this definition, the criteria for admissibility would appear satisfied by, for instance, something as simple as a witness testifying to having received a Facebook message in the "normal manner". This provision seems to invite judicial notice.

Such an approach was recommended by the Albert Court of Appeal in ***R. v. Hogan***, 2022 ABCA 5. In ***Hogan***, the Court of Appeal indicated that a trial judge "is entitled to rely on data that is automatically collected and displayed by instruments in common use, at least in the absence of any formal objection… Smart telephones are

now sufficiently ubiquitous that, in the absence of a specific objection, trial judges are entitled to take notice of their capabilities and the reliability of the information they generate. The inherent reliability of such automatic devices rests in their scientific design and testing, and it is confirmed by the fact that they are routinely used millions of times every day" (at paragraphs 9 and 10).

The Threshold Test Contained Within the Canada Evidence Act:

In ***Durocher***, the Saskatchewan Court of Appeal considered section 31.1 of the *Canada Evidence Act* and held that the "burden of proof to establish threshold authenticity for purposes of s. 31.1 is low and, once satisfied, the document is admissible and available for use by the trier of fact…To meet this threshold, the proponent need only provide sufficient evidence of authenticity from which the trial judge could reasonably find the document to be what it purports to be" (at paragraph 82). Similarly, in ***Richardson***, the New Brunswick Court of Appeal held that the *Canada Evidence Act* determines "how threshold admissibility of electronic documents is determined, not ultimate admissibility. In addition to the threshold statutory requirements, electronic documents — like any other form of document — must satisfy common law rules to support the admission of their contents, such as being legally relevant and complying with rules applicable to hearsay evidence when documents are adduced for the truth of their contents" (at paragraph 24).

It was also held in ***Durocher*** that the presumptions contained in the *Canada Evidence Act* in relation to "electronic documents" are "aimed at providing some assurance that no changes in the information found in the document have been caused by technical reasons or human intervention" (at paragraph 89). One might suggest just the opposite. The presumptions take away the opportunity to make such an argument at the admissibility stage.

As noted earlier, in ***Durocher***, the contested evidence was a series of Facebook text messages said to have been sent by the accused to the complainant (L.A.). The Court of Appeal concluded that these messages were admissible pursuant to the *Canada Evidence Act* because "L.A. provided some evidence capable of supporting a conclusion that [the messages were] what L.A. claimed it to be" (at paragraph 94). What was that evidence? L.A. testified that accused sent her text messages. Thus, they were admissible because the *Canada Evidence Act* mandates that "the integrity (or reliability) of the electronic document is not open to attack at the authentication stage of the inquiry" (***Hirsh***, at paragraph 18).

Document Integrity and Evidence to the Contrary:

The issue of "document integrity", as governed by section 31.1 of the *Canada Evidence Act*, was considered by the Court of Appeal for Newfoundland and Labrador in ***Martin***.

The Court of Appeal held that that "system integrity is an admissibility issue" and an "admissibility requirement" (at paragraph 56). However, the Court of Appeal also held that the test for establishing system integrity is a low one and the Court of Appeal emphasized the importance of the party objecting to the admissibility of social media evidence having the burden of providing "evidence to the contrary".

The Court of Appeal indicated that 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" (at paragraph 60).

The Court of Appeal, in considering section 31.2 of the *Canada Evidence Act*, indicated that a trial judge need only "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" for this element to be established (at paragraph 57).

In ***Durocher***, the Saskatchewan Court of Appeal held that the accused had not presented any "evidence to the contrary", thus, there was no "basis to doubt the integrity of the electronic document system, i.e., L.A.'s smart phone. While defence counsel took issue with whether Mr. Durocher was the author of the Facebook messages at trial, there was no suggestion that the messages might have been altered or tampered with. I am satisfied that the presumption of integrity set out in s. 31.3(a) and s. 31.3(b) of the *CEA* applied. L.A. was never challenged on her evidence and, as such, the presumptions were not rebutted by Mr. Durocher" (at paragraph 95).

Finally, section 31.3 of the *Canada Evidence Act* was also considered by the New Brunswick Court of Appeal in ***Richardson***. In concluding that electronic messages were properly admitted at trial, the New Brunswick Court of Appeal held that "lay evidence that the messaging system was successfully used, and the messages displayed corresponded to what the different witnesses recalled, can form the basis for satisfying the s. 31.3(a) presumption, for this is evidence the computer system, having faithfully reproduced the information, must have been functioning as it should" (at paragraph 46). The Court of Appeal concluded that the "threshold for

authentication" was met because, Mr. Jamieson testified that the accused "was the other person in the MSN conversations" (at paragraph 51).

A Summary:

Authentication requires the introduction of some evidence to establish that the document is what it purports to be. However, this does not generally require proof that the document is genuine or accurate. That is a question of weight not admissibility. Social media evidence can be authenticated even when it is disputed that it is what it purports to be.

It has been pointed out that "to authenticate an electronic document, counsel could present it to a witness for identification and, presumably, the witness would articulate some basis for authenticating it as what it purported to be" (***Hirsh***, at paragraph 18).

Thus, 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 factfinder for ultimate evaluation" (Paciocco, *Proof and Progress: Coping with the Law of Evidence in a Technological Age*, at page 199).

Though the threshold for admissibility is low, any social media evidence sought to be introduced must be relevant, and not subject to an exclusionary rule. This principle is codified in section 31.7 of the *Canada Evidence Act*.

The Social Media Evidence Must be Otherwise Admissible:

Section 31.7 of the *Canada Evidence Act* indicates that 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". Therefore, any social media evidence sought to be entered must be otherwise admissible (see ***R. v. N.P.***, 2021 BCCA 25). As a result, a message sent by social media cannot be used as a prior consistent statement to bolster a witness' credibility (see ***R. v. Lapierre***, 2022 NSCA 12, at paragraphs 96 to 109), though it may be used as narrative evidence to "understand how the complainant's story was initially disclosed" (***Lapierre***, at paragraph 110).

In ***R. v. Singh***, 2021 BCCA 172, it was pointed out that in assessing "text communications between the complainant and the accused" a trial judge "can properly rely on the timing, context, and tone of such prior communications to assess the credibility of both the complainant and the accused" (at paragraph 35). The British Columbia Court of Appeal also indicated that a "text or electronic exchange between a complainant and the accused can have independent cogency. This may be particularly true in the context of sexual assault cases where 'there may be little other

evidence to serve the court in its truth finding mission beyond the testimony of an accused and a complainant'" (at paragraph 37).

The Admissibility of Screenshots of an Electronic Document:

What if a witness takes a screenshot of a Facebook posting by the accused and a party to the proceeding seeks to introduce it as evidence?[3]

This issue was considered by Court of Appeal for Newfoundland and Labrador in ***Martin***. In that case, the accused was charged with a number of weapon offences. At his trial, the Crown sought to introduce into evidence six screenshots depicting posts purportedly taken from the accused's Facebook page. The screenshots purportedly showed the accused holding a prohibited firearm. The screenshots were provided to the police by an anonymous source. Officers testified that they were able to identify Mr. Martin and his apartment as being depicted in the screenshots from having had contact with him and from having been inside his apartment.

The trial judge concluded that the evidence was inadmissible and the accused was acquitted. The Crown appealed from acquittal.

The Court of Appeal described the issue raised in the following manner:

> 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.

The appeal was allowed. The Court of Appeal for Newfoundland and Labrador indicated that Facebook posts "fall within the definition of electronic documents in section 31.8 of the *Canada Evidence Act*" (at paragraph 25). The Court of Appeal concluded that 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" (at paragraph 29).

---

[3] In ***R. v. R.R.***, 2022 ONCJ 158, it was held that screen shots taken of Snapchat messages (which automatically disappear after a period of time) met "the authentication requirements found in section 31.1 of the *Canada Evidence Act*" (at paragraph 14). Similarly, in ***R. v. Alexandre***, 2022 ONCJ 132. it was held that "the use of a photocopier does not affect the authenticity of the documents. When I examine the documents, I am satisfied that they are what they purport to be. That is to say, I am satisfied that they are copies of documents produced by the MTO" (at paragraph 11).

The Court of Appeal held that the threshold requirement for authentication had been established because 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*" (at paragraph 70). Thus, "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" (at paragraph 74).

These comments illustrate how difficult it can be to challenge the reliability of social media evidence once the low threshold of authentication has been met. The placing of the onus on the party opposing admission can create a substantial hurdle.

Conclusion:

As we have seen, the threshold for the admissibility of social media evidence in Canada is a very low one that can be established with minimal evidence. When this is combined with a presumption of integrity, it results in social media evidence being readily admissible in Canada.

In summary, for an electronic document to be admissible in Canada, the party seeking to have it admitted must:

> 1. establish authentication. The test at common law and pursuant to the *Canada Evidence Act* is identical and constitutes a very low threshold: that the document is what it purports to be;
>
> 2. this can be established by a witness describing what the item is, or how it was received or sent;
>
> 3. authentication does not require proof that the document is genuine, only some evidence capable of establishing that it is what it purports to be (i.e., an electronic document);
>
> 4. there is a presumption of integrity in relation to computer systems, as a result of which the party seeking to have an electronic document admitted does not have to establish that the computer system was working properly when the document was created, found or copied; and

> 5. the onus rests on the opposing party to introduce evidence to the contrary when seeking to challenge the integrity of an electronic document.

Authentication of social media evidence involves a low threshold in Canada because it is a threshold issue and because of the nature of modern communications. The ultimate weight is to be assessed in the context of the totality of the evidence presented. As Professor Silver correctly points out, "[t]here is no room in the [*Canada Evidence Act*] regime for the gatekeeper function and once admitted under that regime, the social media evidence faces no further threshold scrutiny" (see Lisa A. Silver, *The Unclear Picture of Social Media Evidenc*e, at page 135).

This is correct, however this type of evidence is subject to the same rules of evidence that apply to other forms of evidence. As a result, admissibility will require more than passing a witness a photocopy and asking them to identify it.