

CANADA / JUDGMENT

R. v. Alkhalil

2022 BCSC 890

COURT

Supreme Court of British Columbia

DECIDED

31 May 2022

Source: bccourts.ca · Research copy typeset by Esheria. Not court-issued or certified.

2022 BCSC 890 R. v. Alkhalil

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:

R. v. Alkhalil,

2022 BCSC 890

Date: 20220531

Docket: 27393-161

Registry: Vancouver

Regina

v.

Rabih Alkhalil (a.k.a. Robby Alkhalil) and

Larry Ronald Amero

Restriction on Publication: A publication ban has been mandatorily imposed under s. 648(1) of the Criminal Code of Canada, restricting the publication, broadcasting or transmission in any way of any portion of the trial at which the jury is not present. This publication ban applies until the jury retires to consider its verdict

Before: The Honourable Justice Maisonville

Ruling re Application No. 161 - Electronic Documents and the Canada Evidence Act

Counsel for the Crown:

M. Sheardown

S. Dworkin

A. Cochrane

N. Gregoire

A. La Bar

Counsel for the Accused, Rabih Alkhalil (a.k.a. Robby Alkhalil):

R.S. Fowler, Q.C.

K. Blok

Counsel for the Accused, Larry Ronald Amero:

M. Rock

J. Oppal

Place and Dates of Trial/Hearing:

Vancouver, B.C.

May 20, 24, 25, 2022

Place and Date of Ruling:

Vancouver, B.C.

May 31, 2022

introduction

- [1] The Crown seeks to lead evidence of PGP encrypted emails obtained from BlackBerry devices with police exhibit numbers 8LW, 9LW, 15LW, 20LW, and PH003 (referred to as the "Nero device" throughout these proceedings). The first four devices were seized from a residence in Montreal (the "Montreal Residence") and are alleged to have been used by either Rabih Alkhalil (8LW and 9LW) or Larry Amero (15LW and 20LW). The Nero device, seized from a residence in Ontario, contains messages from one of the purported PGP accounts of Mr. Alkhalil.
- [2] After the BlackBerry devices were seized by police, their contents were imaged. The images were then processed through RDX software by S/Sgt. Bernier or others with the RCMP's Technical Analysis Team ("TAT") in Ottawa, who then generated extraction reports.
- [3] The Crown seeks an order that the RDX extraction reports for the five BlackBerrys satisfy the authenticity and integrity requirements for electronic documents set out in ss. 31.1 to 31.8 of the Canada Evidence Act, R.S.C. 1985, c. C-5 [CEA]. It submits that the reports amply meet the low threshold required for authentication, as there is evidence capable of supporting a finding that the RDX extraction reports are what they purport to be, namely, an electronic document containing PGP messages authored by either Mr. Alkhalil or Mr. Amero, depending on the device. Further, the Crown says that whether through operation of s.

31.2(1)(a), s. 31.3(a) or s. 31.3(b) of the CEA, the RDX extraction reports satisfy the best evidence rule.

- [4] Mr. Alkhalil acknowledges that given the low threshold, there is some evidence to support both the authenticity and integrity requirements of the CEA. He cautions, however, that s. 31.3(b)--document recorded or stored by a party adverse in interest--is not an available route to establishing the integrity of the documents since it cannot be said that the RDX reports were created by a party adverse in interest.
- [5] Mr. Amero disputes the authenticity and integrity of the RDX extraction reports. He points to several apparent anomalies or discrepancies in the reports, and submits that they are therefore not what they purport to be, an exact representation of the messages sent and received by the BlackBerry device.

Analysis

- [6] Sections 31.1 to 31.8 of the CEA are the governing provisions on this application:

Authentication of electronic documents

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

Application of best evidence rule -- electronic documents

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.

[]

Presumption of Integrity

31.3 For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven

- (a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;

- (b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or
- (c) if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it.

[]

Definitions

31.8 The definitions in this section apply in sections 31.1 to 31.6.

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. (système informatique)

data means representations of information or of concepts, in any form. (données)

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

electronic documents system includes a computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic documents. (système d'archivage électronique)

secure electronic signature means a secure electronic signature as defined in subsection 31(1) of the Personal Information Protection and Electronic Documents Act. (signature électronique sécurisée)

Authenticity

- [7] The burden of proving authenticity rests with the party seeking admission of the electronic document. The threshold for authentication is low: *R. v. Alkhalil*, 2021 BCSC 2220 at para. 47. As noted there, all that is required is some evidence going to the issue of authentication:
- [47] Section 31.1 requires that the Crown establish the authenticity of the electronic documents it seeks to enter into evidence. The threshold for authentication in s. 31.1 is low as recognized in *R. v. Hirsch*, 2017 SKCA 14 at para. 18:

I am not persuaded by Mr. Hirsch's arguments on authentication and the related issue of authorship. In my assessment, s. 31.1 of the Canada Evidence Act is a codification of the common law rule of evidence authentication. The provision 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: The Honourable Justice David Watt, *Watt's Manual of Criminal Evidence*, 2016 (Toronto: Thomson Reuters, 2016) at 104 [Watt's Manual]. Quite simply, 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 (see: *Pfizer Canada Inc. v Teva Canada Limited*, 2016 FCA 161 at para 93, 400 DLR (4th) 723). That is, while authentication is required, it is not an onerous requirement. In Watt's Manual, the author notes at 1115:

The burden of proving 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.]

- [8] Evidence can be authenticated even when there is a contest over whether it is what purports to be: *R. v. Durocher*, 2019 SKCA 97 at para. 84; *R. v. Martin*, 2021 NLCA 1 at paras. 49 to 51. As the Newfoundland Court of Appeal explained in *Martin* (at para. 50):
- [50] Electronic evidence is intangible evidence and its type and use are continuously evolving in our present world. Perhaps because of these factors, the [CEA], 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.
- [9] Authenticity can be established through either direct or circumstantial means: *R. v. Ball*, 2019 BCCA 32 at para. 85; *R. v. C.B.*, 2019 ONCA 380 at para. 68. *Martin* is an example of the use of circumstantial evidence to support a finding of authenticity.
- [10] In *Martin*, the Crown had sought at trial to tender evidence of various screenshots depicting what appeared to be posts from the respondent's Facebook account. The screenshots had been mailed to the police from an anonymous source and officers identified the accused in some of the pictures in the posts. The trial judge refused to admit the posts because no witness had been called to testify that the posts had been found on an authentic Facebook account; nor was there any evidence of authorship or that the posts were unaltered or unchanged. On appeal, a majority of the Court held that the trial judge had erred. The Court wrote (at para. 52):

[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.

[11] Accordingly, it is clear that circumstantial evidence of authorship can inform the query of whether electronic documents are what they purport to be.

[12] Authorship, however, is not to be confused with authentication. In *Durocher*, the Saskatchewan Court of Appeal made the following comments (at para. 85):

Before leaving the issue of authenticity, I wish to briefly comment on the relationship between authorship and authenticity. Although there appears to be some confusion in some of the case authority as to whether authorship is subsumed within the concept of authentication, the better view is that these are two distinct concepts giving rise to two distinct tests: see, for example, *Soh*, *R v Hamdan*, 2017 BCSC 676, 349 CCC (3d) 338 [*Hamdan*], and *R v Moazami*, 2013 BCSC 2398 [*Moazami*]. *Hirsch*, from this Court, speaks of authorship as a related issue to authentication, but it does not say that it is synonymous (at para 18). This conclusion stands to reason since, as explained in *Graham Underwood and Jonathan Penner, Electronic Evidence in Canada*, loose-leaf (Rel 1, 2016) vol 1 (Toronto: Thomson Reuters, 2010), authorship and authentication speak to two different concerns (at 13-11):

It is also important to note that establishing the authenticity of an electronic document is not necessarily synonymous with demonstrating its authorship. The relationship between authenticity and authorship for electronic documents is not reciprocal; demonstrating authorship is sufficient to establish authenticity, but establishing authenticity of an electronic document does not necessarily provide strong evidence of authorship. [Footnotes omitted.]

- [13] Turning to the present case, I am satisfied that there is evidence capable of supporting the finding that the RDX extraction reports for 8LW and 9LW are what they purport to be, that is, electronic documents that contain PGP messages authored by Mr. Alkhalil.
- [14] There is circumstantial evidence linking Mr. Alkhalil to the two devices, as both were found in a bedside table in a bedroom in the Montreal Residence alleged to belong to Mr. Alkhalil. Police located identification in Mr. Alkhalil's name in the room. Moreover, from the same bedside table police seized a further BlackBerry device, police exhibit 3LW, with a memory card containing personal images of Mr. Alkhalil. With respect to 9LW, the police located an SD card inside that contained more personal images of Mr. Alkhalil consistent with his use of the device.
- [15] I am similarly satisfied that there is evidence capable of supporting the authenticity of the RDX extraction reports for police exhibits 15LW and 20LW, which the Crown alleges contained messages of Mr. Amero and other co-conspirators. Circumstantial evidence linking Mr. Amero to these devices includes where they were seized and certain non-encrypted content they contain. 15LW was found on the floor near the bed in the bedroom alleged to belong to Mr. Amero. The device contained non-encrypted accounting notes that correspond with "scoresheets" bearing Mr. Amero's fingerprints and found in a plastic drawer in the same bedroom. Similarly, 20LW was found inside the same plastic drawer and has non-encrypted content such as personal information and images of Mr. Amero. It also contains accounting notes that appear to be authored by the same person who created the accounting notes in 15LW.
- [16] Lastly, there is evidence supporting the authenticity of the RDX extraction report for the Nero device. Various RDX-extracted messages from the Nero device, cross-referenced with other evidence that has been led in the trial, collectively shows that Mr. Alkhalil was the purported author of the messages in question.
- [17] Accordingly, I conclude that the RDX reports for police exhibits 8LW, 9LW, 15LW, 20LW and the Nero device satisfy the authenticity requirements of the CEA.

Authenticity/Best Evidence Rule

- [18] Sections 31.2 to 31.3 of the CEA codify the best evidence rule and set out the requirements for establishing the integrity of electronic documents. The Crown cites three provisions and says it satisfies each of them, though it need only satisfy one to establish the integrity of the RDX extraction reports.

[19] First, the Crown cites s. 31.2(1)(a), which provides that the best evidence rule in respect of an electronic document is satisfied "on proof of the integrity of the electronic document system" that recorded or stored it. The Crown relies here on the evidence of S/Sgt. Bernier given during the expert evidence voir dire about the reliability and integrity of RDX software. A key portion of his evidence on this issue was as follows:

Q Have you ever observed any instances where RDX generated reports were shown to be completely wrong?

A No.

Q Now, with respect to the nature of decryption and encryption, what happens if you don't use the right decryption key?

A You don't get the output. You don't get decrypted output.

Q So if you do get output, what does that mean to you?

A That the decryption key, the secret to the decryption algorithm, was applied correctly and you got the -- the resulting human readable text.

Q So when you do get a report generated through RDX, what does it say to you about whether it successfully decrypted the messages on that device?

A That it worked. That the decryption worked, especially in cases where there are two levels of encryption.

Q Now, as a result of your education, work, and experience, have you formed an opinion about the integrity of the RDX extraction reports produced by formerly known as TAT as to whether they reliably reflect the content of the examined devices?

A Yes.

Q And what's that opinion?

A That it is reliable.

[20] I accept the Crown's submission and find that s. 31.2(1)(a) is satisfied on the basis of the reliability of the RDX software.

[21] Second, the Crown argues that integrity can be presumed under s. 31.3(a), "by evidence capable of supporting a finding that at all material times" the computer system used by electronic documents system was "operating properly" and, if not, "the fact of it is not operating properly did not affect the integrity of electronic document and there are no other reasonable grounds to doubt the integrity of the electronic document system". It says this is known as the "functioning system" presumption.

[22] The Ontario Court of Appeal considered this provision in *R. v. S.H.*, 2019 ONCA 669, and wrote the following:

- [25] In my view, the requirement in s. 31.3(a) of the [CEA] 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.
- [26] Exhibit 3B, when reviewed in the light of officers Ford and Varey's evidence reveals the presence of numerous text messages stored in chronological order and customary format, demonstrating coherent conversations, between a sender and a recipient that had been both sent and received by the Samsung cell phone. The extraction report also indicated that numerous messages had been read by a recipient.
- [27] Further, the conversations on the extraction report are contextually consistent with other facts in this case. For example, there are references to a dog and a pig in the text messages. According to officer Varey's initial evidence, both a dog and a pig were present when the search warrant was executed. No basis for questioning the integrity of the electronic documents system has been suggested on appeal or in the court below.
- [28] In my view, the appellant's arguments that it was necessary that the Crown call C.H. to verify the content of the text messages or provide evidence of testing the Samsung cell phone text messaging system is misconceived. In the context of the evidence adduced in this case, that would amount to requiring that it be established that, at all material times, the Samsung cell phone was operating properly. That is not the threshold under s. 31.3(a).
- [23] I agree with the Crown's submission that the evidence of S/Sgt. Bernier during the expert evidence voir dire, coupled with RDX extraction reports that display readable, coherent, chronologically laid-out messages, and evidence contextually consistent with the other evidence led in the case, satisfies the low threshold in s. 31.3(a) as well.
- [24] Mr. Amero placed into evidence a series of RDX decrypted PGP messages, and referred to S/Sgt. Bernier's testimony with respect to them. In one instance, S/Sgt. Bernier was questioned why a particular message had a July date, which, it was suggested to him, made no sense given that the conversation appeared to have occurred in August. S/Sgt. Bernier was not able to provide an explanation. Another example related to the number of messages a Cellebrite report indicated existed as compared to the RDX report for the same device, the latter being larger. S/Sgt. Bernier was asked how this was possible given that the Cellebrite report should show more messages than the RDX report:

Q So if there's 800 messages, 500 of them PGP, 300 non-PGP, Cellebrite should extract 800, 300 that are readable and 500 that are encrypted.

A That -- yeah, that analysis would have to get done comparing RDX to Cellebrite to confirm that. Cellebrite did have a point in time where they weren't outputting the content of the messages, later on they did, so it's -- it would have to be compared, each extraction.

Q Either content or no content, I'm just talking about numbers. You should have 500 encrypted plus 300 non-encrypted. Cellebrite would extract 800 messages total.

A I would -- I would believe it would be able to, yes.

Q Okay. And the one that are encrypted, even though they're not decrypted you're able to gather some informations on them. For example, the date and time it was sent?

A Yes, the sent date/time.

Q What other information are we able to gather on them?

A The -- the to and the from.

[25] It is clear that the officer's answer was in response to the number of messages only. While Mr. Amero submits that these two examples demonstrate flaws in the RDX extraction reports, I find the answers of S/Sgt. Bernier were nuanced and not simply agreement with defence counsel's statements. No flaw was conclusively established on this application, beyond the level of argument. In any event, given the many thousands of pages of RDX reports that exist, I do not consider these two examples sufficient to detract from the proposition that the document system was operating properly within the meaning of s. 31.3(a). Consequently, I find the functioning system presumption applies to all of the RDX extraction reports in issue.

[26] Having concluded that the Crown has satisfied both ss. 31.2(1)(a) and 31.3(a), it is unnecessary to address the arguments with respect to s. 31.3(b).

Conclusion

[27] For the reasons above, I find that the RDX extraction reports for 8LW, 9LW, 15LW, 20LW and the Nero device satisfy the authenticity and integrity requirements for electronic documents contained in the CEA.

"Maisonville J."

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/sc/22/08/2022BCSC0890.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/r-v-alkhalil-2022-bcsc-890>

Prepared on 28 October 2026 · Esheria