BC Society of Transition Houses

Authentication of Digital Evidence for Family or Civil Matters in BC Courts

Introduction

Digital evidence such as text messages, e-mails, and social media posts are often relevant to family or civil matters in British Columbia courts. As with any piece of evidence to be considered by a court, there are requirements that govern the introduction of all evidence. Authentication is an important step for digital evidence to be admitted by the court.[1] Because British Columbia does not have specific evidence laws about the admission of electronic documents in court, common law principles apply.[2] Common law is based on court decisions and legal precedent.

This information sheet discusses how to authenticate digital evidence for family or civil law matters at the Provincial Court of British Columbia or the Supreme Court of British Columbia.

You can represent yourself in your family or civil law matter. However, if it is possible, it is recommended that you have legal counsel because the rules of evidence can be difficult to understand. Trials and other court hearings can be complicated, and it helps to have a legal expert presenting your case and arguing evidentiary admissibility.

Credibility

Credibility is a fundamental issue for any testimonial evidence presented in court. Credibility is whether the person is believable. Credibility is central to the judge's analysis. The judge will be looking for any conflicts in the presented evidence (for example, two sides providing contradictory testimonies). If two parties disagree on the introduction or authenticity of a document, the judge will consider the credibility of both parties and the evidence offered.

The judge will listen carefully to what each party says in court or submits in written documents. The core of credibility is to tell the truth in court and to be as accurate as possible when providing information and answering questions. Not knowing the answer to a question is okay. You can tell the court that you do not know the answer. If you do not understand a question, you can ask for the question to be repeated or rephrased before answering to make sure you understand it correctly. Only provide answers to the

[1] Unlike Alberta, Manitoba, Nova Scotia, Ontario, Saskatchewan, the Northwest Territories, and Nunavut there are no specific rules in the *BC Evidence Act* for authenticating digital documents in British Columbia. Instead, courts in British Columbia use rules of authentication that have developed through case law.

[2] For examples of BC cases applying common law principles, see *Zhang v Sun*, 2016 BCSC 1418 (65-70); *M(MK) v PSM*, 2013 BCSC 579 (40); *Teunissen v Hulstra*, 2017 BCSC 2365, para 8 and later; *McGarry v Co-operators Life Insurance Co.*, 2011 BCCA 214 (paras 73-76); Sylvestre, quoting from *R v Hirsch*, in which the SKCA stated that the *CEA* sections are a codification of the common law.

question asked. Be clear and direct when testifying, avoid contradictions and argument, and act courteously to all parties.

What Is Authentication?

Authentication requires you to explain to the court that the digital document you are using is what you say it is. For example, the process of authentication of an Instagram screenshot could go as follows: you explain to the court what an Instagram page and app is (i.e., Instagram is an app where users can view each other's photos), how you are familiar with Instagram (i.e., you use it regularly), your Instagram page use (i.e., you post photos to this account), you were the one to take the screenshots of the Instagram page you are wanting to use as evidence, and you were the one to print the screenshot on a specified day at a specified time. If someone else took the screenshot or printed them out for you, they may need to testify at the trial to explain that it was them who collected the evidence.

Authentication of a digital document *requires there to be evidence capable of supporting a finding that the electronic document is what it purports to be. This test, which is stated in* R v Hamdan,[3] *must be met for authentication.*

The phrase ***"purports to be"*** *has the same meaning as "claims to be."*

As mentioned above, you will have to introduce evidence *capable* of showing that the digital document is what you say it is. The word "capable" sets a low threshold for authentication, meaning that it is fairly easy to prove that a document is what you say it is.[4] In some cases, authenticity may not even be disputed, meaning that you may not need to deal with authentication at all. However, it is better to be prepared if the opposing party disputes the authenticity of your evidence or the court has questions.

If the opposing party's evidence seems inauthentic or edited, you can question the authenticity of their evidence in court. The opposing party must then authenticate their evidence for it to be deemed admissible. If the opposing party does not follow the rules of authentication, you can argue that their evidence should be inadmissible on the basis that it has not been authenticated.

[3] 2017 BCSC 676.

[4] *Oswald v Start Up SRL,* 2020 BCSC 205; *British Columbia (Securities Commission) v Alexander,* 2013 BCCA 111.

Authenticating a Document

Since the threshold for authentication is low, as long as there is *some evidence* of authenticity, it may be enough to authenticate the document.[5] Evidence of authenticity is provided through witness testimony.

Who & How

Witness Testimony: Oral or Written

You or another witness must testify that the digital documents submitted to the court are authentic. The testimony can either be an oral testimony given in court or a sworn affidavit. Both forms of testimony are acceptable in certain circumstances. The Supreme Court of British Columbia requires oral testimony for trials and affidavits for applications. The Provincial Court of British Columbia requires oral testimony for both trials and applications, although affidavits can be used for applications if the court allows it.

***Oral testimony** is when a witness answers questions in court under oath.*

***Affidavit** is a written statement sworn under oath. This statement is then submitted to the court.*

Testimony can be used as evidence to authenticate a digital document. To do so, the witness identifies what the document is and provides an explanation to show the document is what they say it is.[6] For example, screenshots of text messages sent to you from an abusive ex-partner may be relevant evidence for your court matter. To authenticate these screenshots, the testimony should explain that the screenshots were taken directly from the witness's phone (i.e., your phone) and accurately represent the text messages that were sent by the ex-partner (i.e., they were not altered in any way). This detailed testimony is usually enough to prove that the document is authentic.

It is best that whoever "created" the digital document (i.e., who took the screenshot, for example) is the one to testify about the document. This is not always required. What is most important is that the witness, testifying about the document, has sufficient relevant knowledge of the event.

If you did not create the digital evidence yourself, you can still provide evidence of its authenticity in certain circumstances.[7] In *R v Hirsh*[8], a woman wanted to show a screenshot of someone's Facebook

[5] *Holden v Hanlon,* 2019 BCSC 622.
[6] *Pfizer Canada Inc. v Teva Canada Limited,* 2016 FCA 161 as cited in *Holden v Hanlon*, 2019 BCSC 622.
[7] *Zhang v Sun,* 2016 BCSC 1418.
[8] 2017 SKCA 14.

profile as evidence at the trial. She was not able to take a screenshot of the profile herself, because the person had blocked her on Facebook. However, her friend was still Facebook friends with the account she wanted to access, so her friend took a screenshot of the account. It was acknowledged during trial that the witness had no way of knowing whether the screenshots had been edited, because she did not take the screenshots herself. The court also acknowledged that it would have been preferable for the friend who actually took the screenshot to testify to the authenticity of the screenshots. However, the court still accepted the witness's testimony because she was familiar with the owner of the Facebook profile: she had access to the profile before she was blocked and was able to recognize the poster's style of writing.

Authenticity *does not* require a third-party (i.e., someone other than you or the opposing party) to testify and authenticate digital evidence. It is generally appropriate for you to authenticate your own evidence if you can truthfully testify to its authenticity under oath.[9]

Incomplete or Edited Digital Documents May Still Be Authenticated

The court does not require you to show that your digital documents are identical to the original digital files. To require this would result in a higher threshold than the one set out in the test for authentication.[10] Again, authentication only requires digital evidence to be what you say it is.

For example, on some social media platforms it is possible to delete sent messages. If an abuser has deleted messages they sent you from your chat, it will be impossible to take screenshots of the "original" conversation because part of it has been deleted. However, you can still screenshot the remaining conversation that has not been deleted. In this case, you cannot claim that the screenshot represents the original conversation because some portion has been deleted. However, you can say that the screenshot accurately represents the remaining portions of the original conversation.

A digital document does not need to be an exact copy of the original digital file; it can be a copy of a modified version of the original file. However, modification of a document should be avoided whenever possible. What is important is that the document is an accurate representation of the information that it claims to show. Thus, you should always carefully review the document that you plan to use in order to clearly and accurately testify that the document is what you say it is. You may have to explain or provide a reason if your digital documents look revised or altered. Your authentication explanation should include that the modified document is an accurate depiction of the original document.

Examples of situations where a digital document may require more explanation include:

- If the document does not include contextual information, such as the time and date of a message.

[9] *Ainger v Posendorf*, 2019 ONSC 2220.
[10] *R v Hamdan,* 2017 BCSC 676.

- If the conversation being captured between two people does not flow logically (for example, if it is obvious that some of the texts have been removed from the document).
- If the document is inconsistent with other documents that are being presented as evidence.

Somani v Jilani[11] is a case where suspicious digital documents were not authenticated. In this case, Mr. Somani attempted to present as evidence a text message printout. The printout in question showed a single text message from Mr. Somani. There was no response to the text from Ms. Jilani. Ms. Jilani argued that she would have responded to the message had she actually received it. This piece of Mr. Somani's evidence was unusual because all other printouts of conversations between Mr. Somani and Ms. Jilani consisted of large volumes of texts – not just a single text. Lastly, Ms. Jilani testified that Mr. Somani was an expert with computers and would likely know how to produce a falsified print out of a text message. The judge found that the printout was suspicious and was not satisfied that it was authentic.

This case highlights the importance of being familiar with your digital evidence so that you can answer questions regarding its authenticity. Additionally, you should try to gather your evidence in a comprehensive and consistent way. This could include preserving the whole text conversation rather than just one or two texts that you think are relevant. This is important in order to present the entire context of a conversation to the court. Establishing a consistent manner of capturing screenshots and gathering documentation will be helpful to show to the court that you have a process you follow in your evidence collection. This can aid in the authentication of your documents before a court.

Anonymous Messages Can Be Authenticated

It is not necessary, *during the authentication step*, to identify the author of a digital message.[12] It often occurs that women are harassed by an anonymous or fake profile. Evidence from an anonymous or fake profile is still admissible in court. At the authentication stage, you only need to show that the screenshots are what you say they are: your evidence, screenshots for example, are an accurate representation of the harassing messages you received from the anonymous or fake account. However, because the author of the harassing messages is hiding behind a fake profile, the screenshot cannot be linked to the true author of the messages. Even if you have a suspicion that the messages were sent by your ex-partner, for example, this is not relevant at the authentication stage.

Forensic digital evidence, like an IP address, that links the fake social media account to an actual person's internet account is not necessary to establish authenticity. At the authentication stage, the author of the digital evidence is irrelevant. Forensic digital analysis may be more important to other

[11] 2018 BCSC 1331.
[12] 2017 BCSC 676.

elements of your court matter, such as identifying the source for the purposes of issuing and serving a court order.

Even though the authentication stage does not require proof of identity, it can be important to a victim's case to identify the person who has been harassing them anonymously. While you may not be able to hire an IT expert to conduct a forensic analysis, you may be able to prove through circumstantial evidence that the anonymous messages came from a specific person. It is important to save digital evidence because it can be helpful to prove the identity of an anonymous harasser. Saved texts or emails from the anonymous account can be compared against the other anonymous messages to show similarities in language or knowledge of private information. These similarities could suggest that the person is an intimate partner or a family member. Similarities between these messages could demonstrate that the same person sent them.

Documents downloaded from third-party applications (apps)

Care should also be taken if digital evidence is being processed through a third-party app, such as an app that backs up or makes recordings of your messages.

In *Sylvestre v Sylvestre,*[13] a printout of text messages using a third-party app was not authenticated. The case details are as follows:

- The witness testified that the printouts "contained downloaded messages from her phone to her computer using the Decipher Text computer app.
- It is not a well-known practice to utilize a third-party app, such as Decipher Text, to authenticate digital evidence. The witness did not explain how the application worked. Thus, there was a gap in explaining how the text messages received on the smartphone were reflected on the printouts from Decipher Text. To close the gap, evidence showing how Decipher Text worked, specifically, how the app converted text messages into printouts, was required. The witness's statements regarding the recorded messages were not sufficient.
- The judge was not able to find that the printouts had been sufficiently authenticated. The judge suggested that, if the witness took screenshots of the text messages herself, instead of using a 3rd party app there likely would not have been a problem with authenticating the digital evidence. The judge also suggested that, for authentication purposes, the witness should have been able to explain how the application worked.

Based on *Sylvestre,* screenshots are preferable than the usage of third-party apps. A screenshot printout is a depiction of what one would see on the screen of a smartphone. Thus, testimony by a witness confirming the accuracy of a screenshot could be sufficient for authentication. There is no need to

[13] 2018 SKQB 105.

provide technical evidence showing how a third-party screenshot is made or how a screenshot printout works. The practice of screenshotting from one's own phone is considered common knowledge for most courts.

However, in certain circumstances, it may be helpful to collect your digital evidence through a third-party app. In cases where there are thousands of text messages or emails, it could be helpful to use a third-party app to print out these messages - rather than screenshot them one by one. It may also be easier to save evidence from social media platforms by using a third-party app due to the high volume of Facebook or Instagram comments.

If using a third-party app, authentication is not overly complex. To the best of your ability, you need to present testimony as to how the application works in a way that is understandable to someone with no prior knowledge of the application. You can testify that the printouts from the application accurately represent the text messages that you received on your phone because you have compared the printouts to the text messages and can confirm their accuracy. This type of testimony may be sufficient for authentication.

Circumstantial Evidence

Circumstantial evidence may be used to determine authenticity of a document as long as that evidence is admissible.[14]

Circumstantial evidence is evidence about the circumstances surrounding an event which may be helpful in proving that an event happened. Circumstantial evidence can be helpful when you do not have direct proof that an event occurred. For example, a person had your phone all day, that person is the only other person who knows your passwords, and a nude photo of you was posted on your Instagram account that day. The fact that he was the only person to have your phone and knew your passwords is circumstantial evidence that they were the one who posted the photo. Circumstantial evidence can be challenged by the other party. They can provide testimony of other circumstances or events to explain the contested evidence.

In *British Columbia (Securities Commission) v Alexander,*[15] the court used circumstantial evidence to determine if documents were authentic. In this case, it was argued that several letters that were submitted as evidence were inauthentic. An individual who was said to have written a letter claimed that he was not in town on the date to have received and responded to a letter. The judge accepted the written letters as authentic after looking at circumstantial evidence:

[14] *British Columbia (Securities Commission) v Alexander,* 2013 BCCA 111.
[15] 2013 BCCA 111.

- The content of the letters showed that the authors were responding to each other (i.e., replying to content contained in the other letters); and
- Credit card statements proved that the individual, who claimed he was out of town when the letters were sent and received, was actually in town on those dates.

Examples of Authentication in Case Law

The following cases are examples where the authenticity of digital evidence was established. These cases illustrate the threshold for authentication in criminal courts. However, these cases can be used in family or civil court matters if the other party tries to argue that you need to meet a higher threshold beyond testimony. These cases would be considered persuasive support for your authentication testimony.

- In *Holden v Hanlon,*[16] a civil matter in BC, both sides at the trial testified to the authenticity of their Facebook Messenger screenshots. Both parties testified about the screenshots, however, neither party was questioned regarding the authenticity of their evidence. The judge found that authenticity was established through their testimonies.

- In *R v Hamdan,*[17] a criminal matter in BC, the testimony of two witnesses who took screen captures of Facebook postings was enough to establish authenticity. They testified that the screen captures they took represented the Facebook pages in question. Both witnesses stated that the digital documents were true and accurate copies of the posts they saw on the Facebook pages.

- In *Ainger v Posendorf,*[18] a family law matter in Ontario, emails were established as authentic after the witness testified that she retrieved the emails from a company computer server by using a password obtained from her son. The witness confirmed that the emails were what she said they were: emails to and from her husband sent while he was working.

How to Challenge the Authenticity of the Other Party's Documents

If you suspect that the other party's documents have been edited or are inauthentic, you can dispute the authenticity of their documents. The burden is on the other party to meet the test for authenticity. You can argue that the other party has not met the test for authenticity that is stated in *R v Hamdan.*[19]

The test requires the party to provide evidence that is capable of proving that their document is what they say it is. If the other party's testimony does not sufficiently explain the context of the digital

[16] 2019 BCSC 622.
[17] 2017 BCSC 676.
[18] 2019 ONSC 2220.
[19] 2017 BCSC 676.

document or how they know that the document is authentic, you can state they have not met the authenticity standard.

It should be raised if the documents have been edited or modified. It may be helpful to submit your own unedited version of text messages, emails, or other social media posts to support the fact that the other party's documents have been altered. Signs of editing may include:

- Incorrect or missing dates and times
- Conversations that do not flow logically
- Documents that are inconsistent with other related documents
- Screenshots which may show gaps in the conversation

If the other party uses a third-party app for their digital documents instead of screenshots, *Sylvestre*[20] suggests that the witness needs to explain how the application works and its reliability. They should also explain how they know that the third-party app accurately represents the original digital file. If the other party fails to do this, it may prevent their documents from being authenticated.

Additionally, you can argue against the credibility of the other party. For example, having a history of submitting false documents or lying about the authenticity of their documents may make the other party less believable.

Finally, circumstantial evidence) might be useful to indirectly show that the other party's documents are not authentic. For example, if the other party tries to submit text message screenshots that are timestamped, evidence that they were at work or otherwise unavailable during that time, could be used as circumstantial evidence. This evidence would show that the other party was doing something else during the time that the messages were allegedly sent. This could help the court infer that the text message screenshots are inauthentic because the other party was working and could not have sent them.

Technology Safety Project

This document is a part of a series that details how to preserve evidence related to the misuse of technology in experiences of domestic violence, sexual assault, and stalking. The series is part of the Preserving Digital Evidence of Technology-Facilitated Violence Toolkit. This document, or any portion thereof, may be reproduced or used in any manner whatsoever as long as acknowledgment to the BC Society of Transition Houses is included in the product.

[20] 2018 SKQB 105.

This document was published March 2021.

We gratefully acknowledge Sherry Xu, JD Candidate, Peter A. Allard School of Law, UBC, support from the Pro Bono Students Canada Organization for the creation of this information sheet. We thank Suzie Dunn of the eQuality Project at the University of Ottawa, Kim Hawkins of Rise Women's Legal Centre and Magal Huberman of Pietrow Law Group for their guidance.

BC Society of Transition Houses

PBSC pro bono students canada réseau national d'étudiant(e)s pro bono