BC Society of Transition Houses

Admitting Digital Evidence in Criminal Court

Rules to Consider

Women[1] who have been targeted by technology-facilitated violence may choose to report those crimes to the police. In a criminal court case, she will be considered a witness to, and a victim of, the crime committed. In this role, she will not have to admit digital evidence to the criminal court herself. Her role will be to tell the police, the Crown counsel, and the court what she experienced and to give her evidence, digital and otherwise, to the police. On some occasions, she will provide evidence to the Crown counsel so that it can be used at trial. It is the role of the Crown counsel to admit evidence to the court about the case.

In criminal cases, the dispute is between the Crown counsel or "prosecutor" who represents the Canadian public, and the accused person, who may be represented by defence counsel or may represent themselves. Complainants, such as the woman who has been harmed by technology-facilitated violence, cannot have a lawyer appear for them at trial or run their own case.

One notable exception to this rule, is in s. 278.4 of the *Criminal Code.* This exception permits a sexual assault complainant or her lawyer to make submissions when the accused person is seeking disclosure of her third-party records (for example, notes from a counsellor). Under this provision, she would only be able to have her lawyer represent her for this one issue at the trial. This is different from family law cases and other "civil" cases, which are between two private individuals. In these cases, either party may have a lawyer represent them or have the option to represent themselves.

Many of the rules for admitting digital evidence in Criminal court are found in the *Canada Evidence Act.* The *Canada Evidence Act* applies to all criminal law cases, and the statute includes important provisions about introducing digital evidence to the court. However, the *Canada Evidence Act* does not provide complete information about how to introduce evidence to a court. It is important to consult a lawyer, or even an evidence law textbook, to fill in the gaps.

For women who encounter the criminal law system as complainants, Crown counsel will introduce all of the evidence, including any digital evidence, against the accused. This means that the woman does not have to self-represent in the same way that she might in a family law case, but nor is she able to control what information the judge receives. Crown counsel does not represent her personal interests, the

[1] In this toolkit we will be using the term "woman", "violence against women" and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. Women and girls face higher rates of most forms of technology-facilitated violence. They also experience some of the most serious consequences as a result of this violence. However, technology-facilitated violence impacts transgender, non-binary, male and female people. We hope that all people impacted by this violence will find these documents useful.

government of Canada, or even the police. Rather, the Crown are supposed to represent the interests of the community as a whole, and "see that justice is done" – whether or not that means a conviction.

In a criminal trial, the complainant needs to act as a witness and provide any digital evidence to the police or Crown counsel. The Crown counsel will determine whether the information is relevant and therefore needs to be given to the defence, and how to enter the evidence into the court record.

For women in this situation, this document may help them to understand the court process and the actions of the Crown counsel and defence. In criminal cases a complainant will not have to introduce the digital evidence to court themselves.

On the other hand, women who enter the criminal law system as an accused person (for example, if they have been accused of a form or technology-facilitated violence) may have to represent themselves if they don't qualify for legal aid and are unable to afford a lawyer. They would have to enter evidence into the court record. For those women, this document can help them understand how they would be expected to admit evidence at their trial.

What is Digital Evidence?

Digital evidence is information that can be admitted to court for a case that is stored digitally or electronically (for example, information that is saved on a complainant's phone, computer, or a website about the crime committed against them). The courts call this type of evidence "electronic document" evidence.

Section 31.8 of the *Canada Evidence Act* defines an "electronic document" as:

> *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, print out or other output of that data.*

Most information that is stored digitally, such as text messages, voice memos, emails, videos, photos, direct messages (DMs), or social media posts, are considered electronic documents. This could include any information that is stored on a complainant's or accused's phone or computer, or on any other form of electronic system or computer. Anything that is stored digitally which can be read, heard, or seen in court may be considered an electronic document. It is not limited to what someone might commonly think of as a "document", such as a PDF or word document. When the Crown prosecutor or defence brings that evidence to court, it will need to be in a format that the court can see and use.

This will likely require the person collecting the evidence to take screenshots or print emails so that they can provide a paper record of the evidence that can be admitted to the courts. If the person collecting the evidence only brings their phone or computer in to show the police or court the evidence on it, it may not be accepted in that form, or they may be required to take that person's phone or computer for

some time to access the evidence. Digital evidence includes printouts of electronic documents. If the person collecting evidence prints out an email or a screenshot of a text, it will generally still be considered digital evidence and would be accepted by the court as such.[2]

Electronic documents have some elements that make them different from non-digital evidence. There are some special rules for admitting digital evidence during a criminal court case. These rules can be found in sections 31.1-31.8 of the *Canada Evidence Act*, which are listed at the end of this document.[3]

Special Rules for Digital Evidence

Before computers were invented and people began saving things electronically, documentary evidence typically had an "original" hard copy, such as a paper copy of the original signed contract or a photo printed from the film of a camera. Judges would want to see a copy of the original in order to have the best version of the evidence in court. This is called the best evidence rule. This rule was made because it was easier to see if changes had been made to an original rather than a copy. If the original wasn't available, the person admitting the evidence would have to explain why they were using a copy, or have a witness explain what the original document contained and why the original copy wasn't being used in the court.

As the world became more digital, the concept of an original document became less relevant. Exact copies of the same document could exist in multiple places at the same time. If someone emailed a photo to another person, both people would have an identical copy of the same photo saved in each of their individual email folders. There was no single, original hard copy. So the courts had to change some of the original rules of evidence to address these differences in digital and non-digital documents.

The evidence rules for "authentication" and best evidence were changed for digital evidence.

Beyond these few special rules for digital evidence, the regular rules for admitting documentary evidence, such as when hearsay evidence is allowed, remain the same - whether the evidence is an electronic document or not.

Authentication

Whoever seeks to admit evidence in court has the responsibility to prove it is "authentic". When the Crown counsel or defence gives an electronic document to the court during a criminal case, the Crown prosecutor or defence will need to authenticate the document by giving the court direct or circumstantial evidence to prove that the digital document is what it purports to be.

---

[2] *R v Ball,* 2019 BCCA 32 at para 75.

[3] *Canada Evidence Act*, RSC , 1985, c C-5.

What this means is that the Crown counsel or defence will have to show that the document they are seeking to admit is what they say it is. For example, if they are seeking to admit screenshots of an Instagram DM where someone has threatened or harassed the complainant, they will need to prove that it is actually a conversation between the complainant and the other person from Instagram. Authenticating evidence can include showing the photo and name of the Instagram profile of the person the complainant was speaking with, as well as a screenshot of their Instagram page to show it is actually them that the complainant was speaking with. They may also need the complainant to tell the court other information that shows she knows the document is what she say it is. The evidence can be authenticated by the complainant saying she has spoken with this person via this account before, she can identify who they are in real life, she is familiar with their account, and she knows how to use that particular social media app or website.[4]

A lawyer or a judge will ask the complainant or another witness to confirm that the document is what it says it is when they are in court and being asked to answer questions about the evidence.[5] In some circumstances, the courts will allow the evidence to be submitted by an affidavit (a written statement where a witness explains what the evidence is and they promise what they said in the statement is true). This is less common and usually only occurs in special circumstances in criminal cases.

The threshold to show the document is authentic is quite low.[6] What this means is that the Crown counsel or defence doesn't have to prove every aspect of the document to show that the document is what it says it is. Some evidence to show that a witness knows the document is real will usually be enough.

Although the threshold is low, there have been some cases where electronic documents were not properly authenticated because it was unclear if they had been tampered with and, as a result, were rejected.[7] For this reason, women should never alter electronic evidence that they have collected.

It is important to remember that, even if the evidence is admitted to the court, it doesn't mean that the judge will believe all of the information in the electronic document. After the evidence is accepted by the judge, the judge will later make a decision about how much "weight" to give the evidence. The judge will decide whether the evidence is trustworthy or relevant to the decision of the case. This may include considering whether the evidence was tampered with or if the account was hacked into.

See BCSTH's Authentication information sheet for more details.

[4] *R v Hirsch*, 2017 SKCA 14 at para 19.

[5] *Pfizer Canada Inc v Teva Canada Ltd,* 2016 FCA 161 at para 93; *R v Andalib-Goortani*, 2014 ONSC 4690.

[6] *R v Hirsch*, 2017 SKCA 14.

[7] *R v Andalib-Goortani*, 2014 ONSC 4690.

Best Evidence Rule

The best evidence rule for non-electronic documents includes showing the original document where possible or explaining why the original document is not available. The best evidence rule is applied when the Crown counsel or defence wants to rely on a secondary document, a copy of a document, or an explanation about a document from a witness, in order to prove something in court.[8]

Because there is usually no true, single "original" document when it comes to most digital evidence, the courts will instead want to know that the system it was saved on was functioning normally.[9] When digital evidence, such as a screenshot from someone's social media page, is submitted as evidence, the courts want to know whether the record *system* (i.e., the phone it was saved on or the social media page it was displayed on) was reliable and wouldn't have altered the electronic document or information wasn't stored inaccurately. The Crown counsel or defence needs to show that the content of the electronic document was properly maintained by providing evidence on the reliability of the system it was stored on.

The complainant or another witness will likely have to explain how the system works (for example, they may need to tell the court the basics about a social media platform, such as how to sign into Facebook, send messages to friends, delete messages, or comment on posts).The relevant witness will need to describe why the platform was working normally when the evidence was created (for example, nothing seemed out of the ordinary when they signed in or checked their messages). In some circumstances, the courts may presume the integrity of a system or platform.

Presumptions of Integrity

When the Crown or defence seeks to admit electronic documents, the court will presume the computer system was reliable if the witness who provided the evidence can prove that it was. If the complainant or another witness can confirm that the system was working normally, the judge will believe that the evidence from the system or social media platform is reliable (i.e., evidence from their phone, email, social media account). Or, if there was a malfunction, the complainant or another witness can confirm that any malfunction didn't impact the reliability of the document.

The court will also presume the admissibility of a document, provided by the Crown counsel or defence, if it is made by someone who is "adverse to the party seeking to introduce it" (i.e., on the other side of

[8] Ken Chase, "Electronic Records as Documentary Evidence" (2007) Canadian Journal of Law and Technology 141 at p 142.

[9] *R v Ball,* 2019 BCCA 32 at para 72-73.

the case to the party admitting it).[10] It will be presumed to be reliable unless proven otherwise in this case.

The document will also be presumed to be reliable if it is a document, made using a routine system by someone who isn't a party to the case, and the person seeking to admit it to court didn't store the electronic document themselves.

However, all of these presumptions can be disputed or proven wrong by the person on the other side of the case. They can bring evidence to show that the system wasn't working, that the information wasn't stored correctly, the information was tampered with, or that the malfunction impacted the reliability of the document. To respond, the other side will have to bring additional evidence to prove the system was working and/or the content is reliable. Otherwise, the evidence may not be accepted by the court.

If one of the presumptions doesn't apply, the Crown counsel or defence will need to provide evidence to prove the integrity of the system.

Canada Evidence Act, RSC, 1985, c C-5.

This section provides relevant sections of the *Canada Evidence Act* that pertain to digital evidence and technology-facilitated violence.

Authentication of Electronic Documents (s 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 (s 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.

Printouts

(2) Despite subsection (1), in the absence of evidence to the contrary, an electronic document in the form of a printout satisfies the best evidence rule if the printout has

[10] *Canada Evidence Act*, RSC , 1985, c C-5, s 31.2.

been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.

Presumption of integrity (s 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.

Presumptions regarding secure electronic signatures (s 31.4)

The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting

(a) the association of secure electronic signatures with persons; and

(b) the integrity of information contained in electronic documents signed with secure electronic signatures.

Standards may be considered (s 31.5)

For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavor that used, recorded or stored the electronic document and the nature and purpose of the electronic document.

Proof by affidavit (s 31.6)

The matters referred to in subsection 31.2(2) and sections 31.3 and 31.5 and in regulations made under section 31.4 may be established by affidavit.

Cross-examination

(2) A party may cross-examine a deponent of an affidavit referred to in subsection (1) that has been introduced in evidence

(a) as of right, if the deponent is an adverse party or is under the control of an adverse party; and

(b) with leave of the court, in the case of any other deponent.

Application (s 31.7)

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

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.

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

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, print out or other output of that data.

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.

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

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.

This document was published March 2021.

We gratefully acknowledge Suzie Dunn and Rachel Sombach of the University of Ottawa and Kim Hawkins of Rise Women's Legal Centre for providing expertise and guidance on the creation of this information sheet.

BC Society of Transition Houses

BRITISH COLUMBIA

THE LAW FOUNDATION OF BRITISH COLUMBIA