BC Society of Transition Houses

Best Practices for Preserving Evidence of

Technology-Facilitated Violence

If you are experiencing technology-facilitated violence, you will want to document what is happening to you. This will help you keep a timeline of what has happened, serve as a memory aid and may be used as evidence if you need to go to court. Because websites can be changed, social media content can be deleted, or people can block you and erase relevant evidence, it is important that you document what is happening to you as soon as it occurs. This could include taking screenshots of texts or direct message (DM) conversations, downloading videos or photos posted of you, recording voice memos, or taking notes of reasons why you think someone might be reading your emails or tracking your movements through your devices.

This guide provides you with practical tips on information you should be collecting and how to document and store that information.

Document, Create a Log and Plan Ahead

When experiencing technology-facilitated violence, itis important to preserve what is happening to you through documentation and to save that documentation in a safe place. Ideally, you will back up the documentation in more than one location, so that if a copy is deleted or lost, you will have an alternative. It can also be helpful to print hard copies of the evidence. If you document the abuse as it occurs and you decide to go to court, you will have evidence of what happened to you in an organized and accessible format.

Step 1: Create a log of what has happened to you

Document all the information that you have access to of the technology-facilitated violence you are experiencing. This includes noting who the perpetrators involved in the abuse are and your relationship with them, the duration of the abuse (i.e., how often it happens and when it started), the impact of the abuse on your life, and any action you have taken, such as asking them to stop contacting or posting about you. You will also want to keep a log of all of the platforms you communicated on (for example, all of the apps, social media sites, messaging apps, phone numbers, etc.) and all of the devices you use (for example, your laptop, your smart phone, your work computer, etc.).

When you become aware of a harassing or threatening message, photo, or video, your first instinct might be to delete it immediately or report it to get it taken down off of the social media website it was posted on. This is particularly true for nude images that have been posted without your consent. However, even though there is a risk that the content might spread if you don't take it down immediately, it is important to collect evidence on the post or image before you delete it or report it to the social media company. If you report it to a social media company and it does break their rules or

terms of service, they may take it down immediately. Once the content is taken down, you may not be able to prove who posted it or that it was ever posted in the first place. It doesn't take much time to document the evidence you need, so it is important to do so before deleting it or reporting it to the social media company. See Step 2 for more information about how to document this evidence.

Once you start collecting information, a documentation log will help keep your evidence organized. You may want to include additional comments where you can include any notes, such as witnesses of particular events, conversations you had with people about the abuse, or messages sent to other people about the evidence.

As you are documenting what is happening to you, you will want to think of what information to collect according to the type of violence which is occurring. For example, you will always want to take a screenshot or a video recording of a threatening chat. But that will not be enough to prove what is happening to you. If you decide to report the abuse to the police or start a civil trial, you will need to prove both what happened to you and who did it. You will also want to show who is associated with the account or phone number that sent or posted the harmful content, the time and date it occurred, and other relevant information. Creating a log of what happened to you, with a list of the information you have collected, can be helpful to ensure you have what you need to prove your case in court.

BCSTH has created a Technology-Facilitated Violence Log which can be used as a template to document your experiences of technology-facilitated violence. If it is safe to do so, you can download the PDF template or read the information on our Technology Safety and Privacy Toolkit webpage.

While gathering evidence, keep an updated collection log that includes the following information for each piece of evidence:

- **Date and time** of the technology-facilitated violent act and when you collected the digital evidence:

  This would include the date and time you received threatening messages and the date and time of when you took a screenshot of the messages. .

- **What happened:** You will want to write down the details of what happened while the event is fresh in your mind. You may remember important contextual details on the day that it happened that may be relevant.

  An important contextual detail would be if your ex started sending you threatening messages after you ran into them at the grocery store with your new partner. That detail might not show up in the chat, but may be relevant to your evidence in court.

- **Evidence that the violence happened** (for example, screenshots of the post): This includes saving copies of what happened to you.

  This may include screenshots of texts or social media posts, emails, or voicemails. Below are examples of how you can document technology-facilitated violence. You will want to save this information somewhere safe, back it up and/or print hard copies of the evidence. It is important to store this evidence somewhere safe. This is especially important if you are worried that the perpetrator has access to your accounts or devices and may be able to delete files or messages from your devices or accounts.

- **Who you think did this**: With the ease of being anonymous on the internet, it is not always clear who the perpetrator is. If you know who it is, you will need to collect information that confirms it actually is that person.

  For example, taking a screenshot of the person's account profile that includes their name, phone number, email address, or photo. If it is not clear from their profile who it is, you should document why you think it is a particular person. For example, if they called you by a nickname they only use to call you, if their identity has been confirmed in a message with a friend, or they said something about you that only they would know.

- **Evidence that the person you suspect did it** (for example, screenshot of their profile in relation to the violence): You will need to show a connection between what happened to you and who did it.

  This could include the screenshots of the perpetrator's profile with their identifying information, such as photos of them, and a screenshot of the threat that shows the person associated with the profile who made the threat.

- **Other relevant information:** There may be additional information you want to keep in your log, such as the name and number of the police officer you reported the violence to (if you reported it), witnesses to the violence and other relevant information.

- **The impact**: You will want to document how the violence has impacted you.

  This could include things such as changes in your behaviour, having to take time off from work or school, feeling fearful and other emotional reactions, needing to confer with health care providers because of health impacts, limiting or closing your social media accounts, blocking people, impacts on relationships, and financial impacts resulting from purchasing new devices and security programs.

- **Evidence still needed:** You may have some gaps in your evidence collection, make a note of it in the log and it will help you remember to collect it later.

Step 2: Collect Evidence

When collecting digital evidence, always remember to collect information related to the person's account or username. Identifying the perpetrator is important for legal proceedings. This includes the email or phone number associated with the account. If the violence occurred in a group chat, you will want to collect the information about each person in the group. You may also want to save information on who "liked" or commented on the content and what was said. Sometimes only a shortened version of a comment will show up in long group chats, so you will want to make sure you open up each shortened version to show the entire message.

Collect the "metadata" associated with the content as well, including timestamps, IP addresses, hyperlinks, or URLs, wherever possible.

Save a digital copy of your evidence, back it up in a second location, and print out a hard copy to store in a binder. Saving the evidence and storing it in chronological order will help document your case and keep you organized. Proving a pattern of abusive behaviour can be supported by this type of detailed and chronological evidence collection. In addition, having a digital copy available is important as it often contains metadata that can be relevant to your case. For example, the screenshots you take often include a date stamp of when you took it.

- **Text Messages:** Take video screen recordings, screenshots or photos of all abusive messages; including the date and time they were received, the contact information of the sender, and the surrounding conversation (your messages included). Courts will often want to see more than just the threatening message and may be interested in the full conversation to understand the context of the message. If the messages cannot be captured in one image, overlap the screenshots halfway to make sure that the full conversation is captured. This will show consistency in the message thread. If you don't overlap your screenshots, the court may wonder if there is any missing information from the conversation. You can also take a video of the message and scroll through the conversation. Make sure you are scrolling slow enough for all the messages to be clear in the video. Be aware some courts may not have the ability to look at or show videos in court, so screenshots are preferable.
- **Videos:** Download videos directly, capture them with a secondary recording device (preferably with a trusted protective application), or use a screen-capture application (such as *Ice-cream Screen Recorder or a video screen recording option on your device*). If you are using a secondary application or program, write down details about the program in case you need to explain to the court how the program works. Then, convert the recordings into a court-admissible format and create physical back-ups (such as on a flash drive) that are password protected. You will need to check with the court your hearings are in to find out what format the recording should be in. Make sure to print out and save a screenshot or a PDF of the webpage where the video was posted, including the URL, date and time of the posting.

- **Voicemail/Calls:** Record all abusive phone conversations and messages by using a recorder app or traditional tape recorder. In Canada, you can legally record a conversation as long as one person in the conversation (i.e., you) consents to the recording, even if the other person doesn't know the conversation is being recorded. Keep your phone records with screenshots, photos, or the log with your monthly bill. In addition, keep a written record of the content of any phone call or message including the date, time, and length of the call. Contact your phone company, alert them to the abuse, you may be able to request their help to monitor the calls, and if possible, have law enforcement send a preservation letter (i.e., a letter that requires the company to preserve evidence related to the abuse) to the company to make sure that their records are not erased. Be aware of potential "spoofing" (use of identity-concealing applications that make it look like the perpetrator is calling from a different number). In addition to keeping a log of any calls from the perpetrator, it is also important to note any patterns that may arise in the abuse, such as specific language or phrases used within the calls or messages.
- **Social Media:** Ask law enforcement to send a preservation letter (i.e., a letter that asks social media companies to preserve data and evidence for a police investigation) to any social media companies whose applications are being used to facilitate violence against you. Always collect information on the perpetrator's profile to show who they are, as well as the other abusive content they sent or posted, and try to capture the date and time the message was posted. Evidence collection specific to each platform is discussed below:
    - **Snapchat:** Capture videos, images and messages sent by the abusive party with a secondary recording device so as to not alert the perpetrator that screenshots have been taken. For example, if you take a screenshot on Snapchat, it will alert the other user, who may then know you are collecting their posts. Snapchat deletes messages, photos, and videos quickly so it is important to capture evidence right away. Keep all of the images and videos sent between you and the perpetrator in a folder, including the timestamp of images sent and received, and the contact information of the sender. It is important to include any photos, videos, and/or messages you send as well, as this presents the evidence in context.
    - **Facebook:** Video screen record, screenshot, take photos of, or print pages that include any harassing images or posts. These "captures" should include the name and profile photo of the poster. You should also capture their profile information, and any interactions that person has had with your posts (including likes/comments). You can also use Facebook's "Information Tool" to receive a full report on all of your activity on the site. You will need to sift through this report to find the relevant information.
    - **Twitter:** Video screen record, screenshot or take a photo of any harassing tweets, as well as the poster's profile info. Then, you may want to report the tweet to Twitter and have copy of the report sent to your email. Keep a record of the tweet's permanent link in a Word document. The permanent link can be accessed by clicking on the hyperlinked

date of the abusive tweet on a computer, and then copying the URL from the search bar. The hyperlink cannot be accessed in the phone app.

- **Instagram:** Video screen record, screenshot, take a picture or a video (with screen capture or an external device) of the abusive post, who posted it (include the person's social media handle at the top of the image), and the date/time of the post. Also, capture the comments section if the abuse continued on the post, or the comments section and context of any posts on your own profile if the abuse extended to any responses on your photos. Include the date you took the picture/video of the post. Make sure to capture the profile of the person harassing you, and the person's profile URL (accessible by clicking the 3 dots next to their username, which can then be saved).

- **E-mails:** Video screen record, screenshot, take a photo of, or print all e-mails between yourself and the perpetrator. Make sure to include the "To", "From", "Subject" and "Date" fields, as well as the header of the e-mail, which contains the IP address. Include any attachments from the e-mail, in addition to the general content. Important note: Do not forward to yourself any evidentiary e-mails, as this will make it harder for the content to be admitted in court. The forwarded e-mail will not contain the original metadata. Metadata is important because it demonstrates that the email came from the perpetrator's account and was received by your email address. You can also contact your e-mail provider to request that they provide backup proof of this evidence.
- **Website:** Video screen record, screenshot, take a photo of, or use the 'Print Page' function to collect evidence of any web-based abuse by saving it as a PDF. If you use the print page function to make a PDF, make sure you double check what was saved, as this function does not always capture the website perfectly. Make sure that the URL of the page, date and time of the post, identity of the poster, and the abusive content is visible. Also, ensure that the date and time of your capture is documented. Save the exact URL of the exact page you are on, as well as the date. You may want to save these details on a separate Word document. You can use this to look up what the page looked like on the date that the abuse occurred by using the archival website, Wayback Machine. However, this archival website is not perfect and it can be difficult to find information on certain websites. It is preferable to take screenshots, rather than relying on the Wayback Machine for evidence preservation.
- **Spyware/ Home Tech:** If you are suspicious that there is spyware on your devices or someone is controlling your Smart technology in an abusive way, keep written records of all suspicious activity. Records should include date, time and description of the occurrences. If possible, keep video and/or photo evidence of the use of this technology (i.e., rapidly changing temperatures in your home, the use of Smart TVs to share abusive messages, the perpetrator knowing private details about your habits or whereabouts, etc.). Records should be kept of all devices that have access to your technology. Additionally, keep a record of any correlated life events that your abuser may know about – such as an anniversary or family reunion – that could contribute to the monitoring behaviour.

Step 3: Protect Your Evidence

Protect your evidence by making multiple copies, saving them in secured digital locations organized by date and time, as well as in a physical evidence binder organized similarly. Make sure to print all pieces of evidence, including images of the webpage where the videos are posted.

If you know or suspect that the perpetrator has the passwords to your accounts, change all of your passwords immediately to a password that the perpetrator would not be able to guess. Changing passwords can be done on your own device, or a device that the perpetrator does not have access to. Some internet browsers, such as Chrome, have a "Save Passwords" function, which can be turned off in the settings. This can prevent your abuser from gaining access to and removing or tampering with your evidence.

Step 4: Report and Remove Content

After capturing all necessary evidence, you may want to report and remove the content where possible. All popular social media platforms provide a "Report" option. This function should be used to notify the platform of the technology-facilitated abuse, and depending on their content removal policies, can result in the company's content moderators removing the post. For websites and posts on webpages, you can also submit a removal form to all search engines, such as Google. This won't take down the website itself, but may remove the content from being searchable through the search engine (Google or Bing). Many of these platforms have content moderation policies that prohibit the posting of non-consensual nude images and other harmful abusive content.

Be aware that once you report the content it may be taken down, so be sure to collect the evidence you need for court before you report the abusive content.

Other Considerations:

- You may want to ask a trusted friend to capture the evidence on your behalf, if you fear that the abuse may persist to the point of being unable to safeguard your evidence. That trusted friend will need to be informed that they will likely need to testify about their involvement in storing the evidence if the evidence is brought to court.
- You may want to ask a friend to keep a copy of the evidence at their home if it is not safe for you to store it with you or if you would feel safer having a secondary copy of the evidence with someone else.
- Ensure that you do not edit any screenshots, photos or videos, as this may make the documents inadmissible in court or result in a judge finding the evidence unreliable.

- When preserving evidence, do not just preserve evidence that you believe is favorable to you. Preserve all evidence that may be relevant to a dispute, including contextual emails, text messages, correspondence, documents, photographs, videos, etc., even if they are embarrassing or show you saying things that are harsh or rude.
- Instead of playing a video or audio recording from a phone, it is better practice to convert all content into an admissible format and put it on an external device (flash drive, CD or DVD). Keep a record of the steps you took to transfer the data from your phone to these devices. The Court Registry should be advised ahead of time to make sure that they have video equipment available in the courtroom to hear this evidence, and inquire what file formats are compatible with their computer systems, if any. Be aware that not all courts will be equipped to accept and show all forms of electronic evidence. They may ask you to provide it in a different form, such as a print out or a transcript.
- With the exception of instant videos such as Snapchat, screenshots are the preferred method capturing evidence, as they keep timestamp records and can be printed for the court.

Preparing Evidence for Court

In order to introduce digital evidence effectively in court, you will want to ensure that it is in an organized and accessible format.

Call the court ahead of time to find out what programs they have to view, hear, or see your evidence, and to make sure that they have the necessary equipment available in the courtroom. Make sure your evidence is saved in a file format that the court is able to use. Even if you can use a screen, you should still bring four paper copies of documents wherever possible (one for you, one for the opposing party, one for the judge, and one for any witnesses to review while they are on the stand).

For screenshots, you may want to have both printed copies and digital copies saved on a USB. Make sure that the information stored on the USB is compatible with the court's computer systems.

Additional Resources

A variety of organizations have developed their own tool kits or tip sheets related to technology-facilitated violence that you may find helpful. When reading these guides, be sure to note what country or province they were published in. If it is from an organization located in a country or province that you don't live in, the laws, evidence rules, and court systems may differ from where you live. However, the practical tips on how to preserve evidence will be helpful across jurisdictions.

BC Society of Transition Houses

"Technology Safety"

https://bcsth.ca/projects/technology-safety/

"Tech Safety Toolkit"

https://bcsth.ca/techsafetytoolkit/

New York Cyber Sex Task Force

"Combatting Cyber Sexual Assault Manual" (American laws but good tips on digital evidence preservation)

National Network to End Domestic Violence (USA)

"Legal Systems Toolkit"

https://www.techsafety.org/legal-toolkit

"Documentation Tips"

https://www.techsafety.org/documentationtips/

WITNESS

"Video as Evidence Basic Practices"

https://www.witness.org/portfolio_page/video-as-evidence-basic-practices/

"Basic Practices: Capture, Storing and Sharing Video Evidence" [Appendix B]

https://library.witness.org/product/video-evidence-basic-practices-capturing-storing-sharing/

"Developing a Collection Plan" [Appendix C]

Badass Army

"Get Help"

https://badassarmy.org/gethelp/

National Council of Juvenile and Family Court Judges

"How to Gather Technology Abuse Evidence for Court"

https://www.ncjfcj.org/wp-content/uploads/2018/02/NCJFCJ_SRL_HowToGatherTechEvidence_Final.pdf

Australia's eSafety Commissioner

"Collecting Evidence of Adult Cyber Abuse"

https://www.esafety.gov.au/report/adult-cyber-abuse/collecting-evidence

"Collecting Evidence of Cyberbullying"

https://www.esafety.gov.au/report/cyberbullying/collecting-evidence

Without My Consent

"Evidence Preservation"

https://withoutmyconsent.org/resources/something-can-be-done-guide/evidence-preservation/

TrollBusters

"Are You Being Harassed Online?"

http://www.troll-busters.com/

Endtab.org

"Deepfake Victim Guide"

https://static1.squarespace.com/static/58b8cb1846c3c4543ab7b863/t/5dcb1ede16bdca031cccb4ff/1573592805299/EndTAB+Deepfake+Victim+Guide+1.0.pdf

Global Investigative Journalism Network

"How to Save Evidence and Why It Matters: Part 1"

https://gijn.org/2016/03/07/how-to-save-online-evidence-and-why-it-matters-part-one/

"How to Save Evidence and Why It Matters: Part 2"

https://gijn.org/2016/03/08/how-to-save-online-evidence-and-why-it-matters-part-two/

Law Technology Today

"Six Best Practices for Capturing Social Media for Use as Evidence in the Court of Law"

https://www.lawtechnologytoday.org/2018/02/six-best-practices-capturing-social-media-use-evidence-court-law/

Removal guides

Cyber Civil Rights Initiative

"Online Removal": https://www.cybercivilrights.org/online-removal/

Stillio

"How to Archive Website: The Ultimate Guide**":** https://www.stillio.com/how-to-archive-website

---

Technology Safety Project

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.