Preserving Digital Evidence

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

Preserving and Storing Evidence of TFGBV: Best Practices

If you are experiencing technology-facilitated gender-based violence (TFGBV), 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 possible after it occurs. This could include taking screenshots of texts, emails, 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 practical tips on information you should collect and how to document and store that information. For specific information regarding how to preserve various forms of evidence, see:

- Preserving Digital Evidence via Video Screen Recording
- Preserving Digital Evidence via Screenshot
- Preserving Video Recordings as Digital Evidence
- Preserving Audio Recordings as Digital Evidence
- Preserving Websites as Digital Evidence
- Preserving Emails as Digital Evidence

Before capturing and preserving digital evidence of abuse, you should always consider whether doing so could pose a risk to your safety. See Safety Considerations for Preserving Digital Evidence and consider contacting an anti-violence organization to discuss safety planning before capturing evidence. See Legal and Victim Service Supports and Resources.

Document, Create a Log, and Plan Ahead

When experiencing TFGBV, it is important to document what is happening to you and to save that evidence in a safe place. Ideally, you will have backup versions of the documents saved 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, you will have evidence of what happened to you available in an organized and accessible format if you decide to go to court.

You may need to show a combination of messages, posts, voicemail recordings, and more to explain to law enforcement, judges, and lawyers what has been happening to you. You may want to keep a text document, spreadsheet, and/or binder that organizes the evidence in one place. Keeping the evidence stored and organized can provide a clear timeline and help explain, to police and the legal system, the details of the violence or abuse.

Collecting and organizing digital evidence is helpful to:

- Provide a record of what is happening, which is useful in pursuing legal remedies
- Alert you to any escalation or change in abusive behaviours such as an increase in monitoring, which may indicate that the situation is becoming more dangerous and your safety plan may need to be revised
- Assist in seeing patterns in the technology-facilitated violence and determine, in detail, how perpetrators misuse technological devices and if there has been a breach of your online security

Step 1: Create a Log of What has Happened to You

Document all the information relating to the TFGBV you are experiencing that you have access to. This includes noting who the perpetrator(s) 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 (e.g. apps, social media sites, messaging apps, phone numbers) and all of the devices you use (e.g. laptop, smartphone, work computer).

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 have it removed from the social media platform or website. 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 it isn't taken down immediately, it is important to collect evidence of the post or image before you delete it or report it. If you report it to a website or social media platform 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 or reporting harmful content. 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 collect information according to the type of violence that 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. Therefore, you will want to record evidence of 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.

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

- **Date and time** of the abusive act and when you collected the digital evidence: This includes the date and time you received the threatening messages and the date and time when you took screenshots of the messages.
- **What happened:** Write down the details of what happened while the event is fresh in your mind. You may remember important contextual details that may be relevant.|

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

- **Evidence that the violence happened**: This includes saving copies of what happened to you. This may include screenshots of texts or social media posts, emails, or voicemails. You will want to back them up and/or have 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 them.
- **Evidence identifying the poster/sender**: 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 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 only they use, if you refer to them by their name and they respond to it, or if they said something about you that only they would know.

- **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 or 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 or security programs.
- **Evidence still needed:** You may have some gaps in your evidence collection. Make a note of these in the log and it will help you remember to collect them later.

You can use this Technology-Facilitated Violence Log as a template to document your experiences of technology-facilitated violence. If it is safe to do so, you can download the PDF template.

Step 2: Collect Evidence

If the evidence you are seeking to preserve includes sexual images of a person under the age of 18 (even if that person is you), **do not screenshot, download, or save the image**. Instead, contact the police immediately. Such images may be considered child pornography.

Capturing a full account of the available and relevant evidence is preferable, as a complete record of the evidence is often required for it to be considered reliable in court proceedings. Partial records, such as a screenshot of a portion of a text message conversation, can be subject to questioning and scrutiny as to why the entire piece of evidence (i.e. the whole conversation from that day) was not presented. For example, a lawyer for the other party may ask you why you only saved one text and imply you may be hiding something by not saving the whole conversation. Preserving and presenting the whole conversation allows the court to see the entire context.

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 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.

If the perpetrator has posted the image online anonymously, it may be more difficult to prove the perpetrator's identity. In a criminal proceeding, the police may be able to get a warrant to obtain identifying information from a website, Internet Service Provider, or social media platform. In a civil proceeding, you may be able to get an order from the court to get this evidence. This, however, can both be costly and time-consuming, and almost impossible if the domain where the information is stored is not based in Canada. In such cases, it will be important to gather as much additional circumstantial evidence as possible to prove the identity of the perpetrator. For information on the type of details that may be relevant to identifying an anonymous perpetrator, see Authentication of Digital Evidence.

When you are collecting digital evidence, it is important to keep in mind the following:

- Capture the entire post or message including the account owner/sender's name, available contact information, date, and time (if available).
- Make sure to collect information that ties the perpetrator to the technology-facilitated violence, such as their phone number, social media profile, or email. You will need to be able to identify the person posting the content in case the court or law enforcement wants to question them.
- Consider creating a new email account that you only use for conversations with the perpetrator. This can help keep track of all conversations.
- If communicating via email, start new email threads with new subject lines regularly. This can help streamline conversations and avoid irrelevant conversations from having to be submitted as evidence.

A copy of all of the communication that identifies the perpetrator, their contact information, and their abusive behaviour can be helpful in legal cases regarding harassment and stalking (see Legal Remedies for Online Stalking, Harassment, Spying, and Threats). This type of digital evidence can show a pattern and series of repeated events. Capturing the whole conversation can also give law enforcement a better understanding of what other evidence needs to be investigated.

Where possible, collect the "metadata" associated with the content as well, including timestamps, IP addresses, hyperlinks, or URLs, wherever possible. Some text and instant message apps do not show the date and time of a message sent and received on that current day. If this is the case, consider preserving the message again the following day so the date and time stamp is visible.

For some social media platforms, instant messaging services, voicemail messages, and text message plans, digital evidence of harassment, threats, and distribution of non-consensual intimate images are only available for a short period. For example, once the platform receives a complaint about the post, it might remove the comment or photo before you have a chance to take a screenshot to show what was posted. Further, the account holder may block you, which means you will no longer have access to the messages or digital evidence. Perpetrators may also realize they should not have said what they did and delete the post before you have a chance to make a copy.

Though it may be difficult to do, it is important to capture digital evidence of violence before it is removed or deleted.

When considering safety, be aware that some apps like Snapchat notify the account holder that a screenshot has been taken of that post or conversation. It may therefore not be safe for you to take screenshots of such content, especially if you are concerned that the perpetrator's violence may escalate if they believe you are collecting digital evidence. You should look up the policies and practices of a social media company before taking screenshots to minimize this risk. If the program does alert the other user to screenshots, you should consider taking a photo of the post with another phone or recording device so the alert function is not triggered.

Digital evidence, such as photographs of physical injuries or recordings of a harassing or threatening voicemail message, can be very important to proving a case in court. It can be helpful to have a friend or other support person document and save evidence of violence. Having others record, preserve, or transcribe digital evidence may not only be necessary to show what violence you are experiencing but may also be a strategic option to keep you safe. If the digital evidence has been taken, stored, or transcribed by a third party such as a friend, that friend may need to testify in court as to their actions and the digital evidence they preserved and possibly submit an affidavit.

> #***TechSafetyTip*** *Have a friend or other third party document evidence of abuse on social media, websites, etc., if it is safe to do so.*

Be cautious when accessing an email or cloud storage website with a web browser. By default, web browsers keep a browsing history.

> #***TechSafetyTip*** *Delete your browsing history after visiting any online sources you are gathering evidence from.*

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. There is no need to highlight, edit, crop, or reformat digital evidence. The courts often want to see the original document without any alterations. If there are alterations, it can cause problems with getting it admitted to court.

When preserving evidence, do not just preserve evidence that you believe is favourable to you. Preserve all evidence that may be relevant to a dispute, including contextual emails, text messages, correspondence, documents, photographs, and videos, even if they are embarrassing or show you saying things that are harsh or rude.

Below are summaries of best practices for preserving specific types of digital evidence.

- **Text Messages:** Take video screen recordings, screenshots, or photos of all abusive messages. Include the date and time they were received, the contact information of the sender, and the surrounding conversation (your own messages included). Courts will often want to see more than just the abusive message(s) and may be interested in the full conversation to understand the context. 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 screen recording of the conversation by slowly scrolling through the

messages. Be aware that some courts may not have the ability to look at or show videos in court, so screenshots are usually preferable.

- **Videos posted online or sent via message:** Download videos directly, capture them with a secondary recording device (preferably with a trusted protective application), or use a screen capture or screen recording application. If you are using a secondary application or program, write down details about the program in case you need to explain how the program works to the court. 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 to find out what format the recording should be in. If the video was posted to a webpage or social media account, make sure to print out and save a screenshot of the webpage where the video was posted, including the URL, date, and time of the posting.
    - **Videos you have made:** In some cases, you may wish to film instances of abusive behaviour using your phone or another camera to use as evidence in legal proceedings. Please note that secretly-recorded videos may not be admitted or may give the judge or jury an unfavourable impression of you.
- **Voicemail/Calls**: Record all abusive phone conversations and messages by using a recording application 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. However, in some circumstances secretly recording a phone conversation may cause a judge or jury to have an unfavourable impression of you. Keep copies of your phone records with screenshots, photos, or the log from 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. If you want the assistance of your phone company in monitoring the calls, you can contact them and alert them to the abuse. You can also have the police or RCMP send your phone company a preservation letter, which is a letter requiring the company to preserve their records of calls between you and the perpetrator. Be aware of potential "spoofing" (i.e. the 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:** You can 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 abusive content they sent or posted, and try to capture the date and time of the posts. If you have been blocked from accessing a perpetrator's account, you may consider asking a trusted contact who has access to their account to collect this evidence, provided you feel this can be done safely. Evidence collection specific to a variety of social media platforms is discussed below:
    - **Snapchat:** Capture videos, images and messages sent by the abusive party with a secondary recording device (such as a second cell phone filming the screen of your phone). **If you take a screenshot on Snapchat, it will alert the 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 picture 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 platform. You will need to sift through this report to find the relevant information. After this is done, you may want to report the posts to Facebook and have a copy of the report sent to your email.
    - **Twitter:** Video screen record, screenshot, or take a photo of any abusive tweets, as well as the poster's profile info. Then, you may want to report the tweet to Twitter and have a 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 Twitter phone application.

- **Instagram:** Video screen record, screenshot, or take a picture or a video (with 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 there. Include the date you took the picture/video of the post. Make sure to capture the profile of the person who posted the harmful content 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. It is always best to print or save the original e-mail rather than a version of the e-mail that you have forwarded to another account or person. When you forward an email, the original metadata is lost. Metadata is important because it shows that the email came from the perpetrator's account and was received by your email address. If you plan to rely on a version of an e-mail that you have forwarded to yourself or someone else, this may raise questions about authenticity. You can also contact your e-mail provider to request that they provide backup proof of this evidence.
- **Websites**: 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 or printing out a physical copy. 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 abusive content are visible. Also, ensure that the date and time of your capture are documented. Save the exact URL of the exact page you are on, as well as the date. You may want to save these details in a separate Word document. If information that was available on a website has now been removed, you may be able to access it using the Internet Archive tool, but this will not work in every case.
- **Spyware and Home Tech**: If you suspect that there is spyware on your devices or that someone is controlling Smart technology in your home in an abusive way, keep written records of all suspicious activity. Records should include the date, time and description of the occurrences. If possible, keep video and/or photo evidence of the use of this technology (e.g. 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). 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.

Many forms of technology-facilitated harassment will involve an abuser posting images of you online on a website or social media. If you have a copy of this image (for example, if you originally sent it to the perpetrator) or if you download a copy of the image, you may be able to determine if the perpetrator has posted it elsewhere through a reverse image search. You can go to Google Images and in the search bar select "Search by image" by clicking on the camera icon. You may then select any image you have saved on your hard drive and run a search for other locations where that image has been posted online. **Please note that it is not clear whether Google can or chooses to retain a copy of an image that you search with**. Bear this in mind in deciding whether or not you wish to run a reverse image search for your intimate images.

Step 3: Store and Protect Your Evidence

Save a digital copy of your evidence, back it up in a second location, and/or print out a hard copy to store in a binder. Depending on the device you are using, video screen recordings, videos, photos, screenshots, and audio recordings will automatically be saved in your photo album, gallery, hard drive, or audio files. 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 them.

Once digital evidence has been preserved, it is important that it be saved somewhere safe. For example, your safety may be at risk if the perpetrator still lives with you and can access your smartphone, uncovers saved recordings, or has your login ID and password to an email address or cloud storage account where you are planning to store the evidence. Ideally, you should save copies of digital evidence in as many safe locations as possible. This may include on your devices, on external hard drives, on friends' or relatives' devices, using "decoy" applications, or using Cloud storage. All of these options come with benefits and with potential safety risks. For more information about how to safely store digital evidence, see: Safety Considerations for Preserving Digital Evidence. You should also consider connecting with a local anti-violence organization if you are experiencing ongoing abuse and are concerned the perpetrator can access your accounts or devices. See Technology Safety and Victim/Survivor Resources for a list of available resources.

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 search engines, such as Google or Bing. This won't take down the website itself but may remove the content from being searchable through the search engine. 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**.

Step 5: Preparing Evidence for Court

To introduce digital evidence effectively in court, you will want to ensure that it is in an organized and accessible format. For more information on preparing and submitting your evidence in court, see: Submitting Evidence in Court; Authentication of Digital Evidence; and An Overview of Canadian Courts.

In criminal proceedings, it will be Crown counsel, not you, who will need to prepare the evidence for presentation in court. However, the Crown can only provide the evidence you give them, so it is important to make sure that all evidence has been captured and stored fully and correctly. In civil proceedings, if you are not represented by a lawyer, you will need to present your evidence to the court. For more information about your responsibilities for presenting evidence in court, see Legal Representation: An Overview and Submitting Evidence in Court.

Some general best practices to keep in mind include:

- Call the Court Registry ahead of time to find out what devices or software they have to view or hear your evidence. You must make sure your evidence is saved in a format that can be viewed in court and that the necessary equipment will be available on the day of your hearing.
- Even if computers, DVD players, or other devices are available, it is always best to bring paper copies of documents whenever possible. You should have four copies of each document (one for you, one for the opposing party, one for the judge, and one for any witnesses to review while they are giving testimony).
- Instead of playing a video or audio recording from a phone, it is a better practice to convert all content into an admissible format and put it on an external device (e.g. USB drive, CD, DVD). Keep a record of the steps you took to transfer the data from your phone to these devices.
- If you are not able to print out the evidence (e.g. voice or video recording), you may need to have the digital evidence transcribed by a third party (i.e. have someone else type up exactly what was said so it can be printed for the court).

Working with a Legal Advocate or Lawyer

Technology-facilitated violence can form the basis of a variety of legal claims (see the Legal Remedies Toolkit for more information). It can be difficult to know what evidence might be relevant for various legal matters. If possible, it can be useful to seek support from the legal community. Legal advocates, lawyers, and law enforcement can help to identify and consider what digital evidence should be collected and what remedies might be available. Additionally, they can help identify what laws may apply that either:

- Directly address the violence and abuse;
- Explicitly or implicitly include the use of electronic communications; or
- Relate to technology, communications, privacy, and confidentiality, even if they are not necessarily focused on underlying domestic violence or sexual assault.

For a list of available legal resources, see Legal and Victim Service Supports and Resources.

Working with Law Enforcement

When reporting a crime, you may not know what information to share, or you may be concerned about giving the police access to private and potentially embarrassing information. Law enforcement departments have policies and protocols for collecting evidence. You should have a conversation about this process with law enforcement before handing over your digital or other evidence. For example, if a technological device, such as a smartphone, is provided to law enforcement for examination, you can ask what information they will be taking from the phone (i.e. downloading a copy of all information from the phone or only taking select photos and conversations), whether the device will be returned, and when.

> **#TechSafetyTip** Have a conversation with law enforcement about what digital evidence is useful, why, and how it will be collected, before turning over your digital evidence or device.

If your digital device is considered a piece of evidence, the police may need to keep it for some time. You may not have access to your devices or online accounts for a short or long period of time, which could have a direct impact on your safety and your ability to communicate with your family, friends, and support network. This possibility should be discussed with an anti-violence worker and become part of the technology safety plan.

> **#TechSafetyTip** Work with an anti-violence worker, where possible, to help you navigate your interactions with law enforcement and come up with a safety plan if your digital devices or accounts have to be turned over to law enforcement.

Meeting with law enforcement can be a highly stressful experience, particularly if you or members of your community have been harmed or traumatized through interactions with law enforcement in the past. Black, Indigenous, and people of colour who have historically been discriminated against and disadvantaged in their interactions with the police might find the prospect of relying on the police in response to technology-facilitated violence to be particularly problematic. If reporting technology-facilitated violence to the police is not a desirable option for you for any reason, you should consider contacting an anti-violence organization to consider your options (see: Technology Safety and Victim/Survivor Resources). Even if the perpetrator's behaviour is a criminal offence, **it is not necessary to report it to the police** and there may be legal remedies available outside of the criminal justice system (see options in the Legal Remedies Toolkit).

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a

shelter/transition house near you or call/text the Kids Help Phone to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

We gratefully acknowledge Moira Aikenhead for providing expertise to update this toolkit and Suzie Dunn of The eQuality Project at 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.

Adapted with permission from BCSTH's Technology Safety project, based on their resource Best Practices for Collecting Digital Evidence of Technology-Facilitated Violence and How to Back Up and Store Evidence of Technology-Facilitated Violence.

Preserving Digital Evidence Example: Sexual Images Shared Online

This document provides an example of what technology-facilitated gender-based violence (TFGBV) might look like and what steps you can take when faced with this violence to preserve relevant digital evidence. For specific information about the legal remedies available to you when faced with TFGBV and specific methods for preserving digital evidence, see the other documents in the Legal Remedies Toolkit and the Preserving Digital Evidence Toolkit.

Scenario

Imani and Jeff dated for two years. During their relationship, they enjoyed sexting and sharing sexual images with each other. Sometimes they made videos of the two of them having sex. They both promised not to share the images with anyone else, and told each other this was something special, just for the two of them. This was really important to Imani because her parents were religious and would not approve of her having sex before marriage. Imani did not share her parent's beliefs about sex before marriage but she also did not want to rock the boat and did not want them to know she was sexually active. She knew if they found out it could really damage her relationship with her family, which was very important to her. Jeff knew that she was always worried her parents would find out they were having sex.

Over the years, Jeff started being more and more controlling over Imani so she eventually tried to break up with him. He said that if she left him, he would send the pictures and videos to her parents. Imani did not want to stay in the relationship with him and didn't know what to do. Jeff said they had to have sex at least one more time or he would share the videos. Imani told him she did not want to but she would do it to stop him from sharing the videos. After they had sex for the last time, she told him their relationship was over. A few days later, she got a call from her friend Micha telling her that a video of her and Jeff having sex was up on a pornography website with her name in the title of the video and that Jeff had sent the link to a group chat on Facebook that Micha, Jeff, and several other friends were in, saying some really rude things about her. Imani is worried that he may post more of the images online and that her parents will find out about the video on the website.

Digital Evidence Collection

In this case, Jeff could be charged with several criminal offences including extortion, the non-consensual distribution of intimate images, and sexual assault. Alternatively, Imani may be able to sue Jeff for breaching her privacy and intentionally inflicting mental distress. For detailed information about possible legal remedies in cases of image-based abuse, like the scenario set out above, see Legal Remedies for Image-Based Sexual Abuse.

Imani's first instinct may be to make a report to the pornography website where the video was posted to get it taken down as soon as possible and to confront Jeff or block him on social media. Before she does either, she should collect as much evidence of the abuse as possible. If she reports the video, the website operator could take it down, making it harder to prove in court that Jeff shared it. If she blocks Jeff or confronts him, he may take the content down. Once she has collected the evidence she needs, she can then consider any necessary steps to have the content removed from the Internet or to communicate with Jeff. Throughout, she should be mindful of any risks to her safety that might result from contacting Jeff or collecting this evidence. See: Safety Considerations for Preserving Digital Evidence.

Below is some general information about the types of evidence Imani should try to preserve. For more information, see Preserving and Storing Evidence of Technology-Facilitated Violence: Best Practices and the guides on preserving certain types of digital evidence linked below.

Evidence from Her and Jeff's Previous Communications

- Imani should look back at all of her text, email, and social media conversations with Jeff and take screenshots or make a screen recording of conversations where they had agreed to keep the images and videos they shared in their relationship private.
- She should take a screenshot of any conversation they had about the video, such as when it was made, who made it, if they shared it with each other and the conversations they had around the video, even if it might feel embarrassing to show the court because of its sexual nature.
- She should take screenshots of any conversations they had where Jeff was upset about them breaking up and when Jeff told her they had to have sex again or he would share the photos or videos.
- She should take screenshots of any conversations they had where she told Jeff that it would be really upsetting for her if her parents found out that she was having sex before marriage.
- Imani should make sure that she collects not just screenshots of the conversations, but information that shows the dates and times of these conversations as well as Jeff's profile information or contact information to show that the person who sent her those messages is actually Jeff. For example, his contact information on her phone will list the phone number that is associated with his cellphone account, which could prove it was actually him sending the messages.
- She should save a copy of the original video, if she has a copy saved on her phone or hard drive.
- If she chooses to delete Jeff from social media or block his number, she should make sure she has downloaded all of their relevant communication beforehand. Some social media companies prevent you from accessing messages between you and a person once you are no longer following each other.

Evidence from Her Friend Micha

- She should ask Micha to take a screenshot of the group chat message Jeff sent, including screenshots that show who is in the group, the post with the link, and Jeff's profile or contact information related to his account. Imani will need to be able to prove not only that the link was posted to the group, but that it was Jeff who posted it. If Jeff uses a fake name or nickname on his profile, it will be important to collect other evidence that would show that Jeff uses that account, such as other posts on the account that have his photo or other information that could prove it is his account. This information should be collected right away, as Jeff may delete it later.
- She should ask Micha for a copy of the link to the video that Jeff sent the group.

Evidence from the Pornography Website

- Imani should take a screenshot or screen video recording of the video on the website. If there is information about the date, the user who posted the video, and how many times it has been viewed, she should screenshot that information, including whatever details she can get about the user's profile.
- She should take a screenshot of what the video was titled by the poster, and also write it down.
- She should copy the URL of the video and save it in a separate document.
- She should take a screenshot of the length of the video.
- She should take a screenshot of any comments that are posted on the video.
- If there is any information that could link the posting back to Jeff, such as the username of the account that posted the video or the wording in the title of the video, she should document that. In many cases, images and videos are posted anonymously or under a fake name so it is more difficult to prove in court who posted them. Imani should collect whatever information she can. In some cases, the police or the courts may be able to get a court order that will order the website owner to provide more information about that particular account that can help identify who was associated with the user who posted the video.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you or call/text the Kids Help Phone to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

We gratefully acknowledge Moira Aikenhead for providing expertise to update this toolkit and Suzie Dunn of The eQuality Project at the University of Ottawa for providing expertise and guidance on the creation of this information sheet.

Adapted with permission from BCSTH's Technology Safety project, based on their resource Collecting Digital Evidence For Your Case: Fact Scenarios.

Preserving Digital Evidence Example: Online Harassment

This document provides an example of what technology-facilitated gender-based violence (TFGBV) might look like and what steps you can take when faced with this violence to preserve relevant digital evidence. For specific information about the legal remedies available to you when faced with TFGBV and specific methods for preserving digital evidence, see the other documents in the Legal Remedies Toolkit and the Preserving Digital Evidence Toolkit.

Scenario

Grace and Yael are in the middle of a heated custody battle over their son. Grace has been sending Yael texts and emails every single day, some of which she sends in the middle of the night. Some days, it is more than 100 texts. Grace's messages are sometimes about their legal issues and arranging drop-offs and pick-ups for their son, but a lot of them are Grace going on about the reasons she is upset that they broke up. Others are calling Yael names, saying she is a bad person and that Grace is going to "get her" if she takes away their son. Some of the texts that Grace sends have information that Yael never gave to her, and Yael is worried Grace might have hacked into her email. Yael has asked Grace to stop texting her so much and to only text her about their son.

Recently, Grace's behaviour has escalated. Grace has been posting awful things about Yael on Facebook, saying that Yael is a terrible mother and is using the courts to turn their son against Grace. She has been following Yael and their son and filming them with her phone while they are at the park, yelling at them that she is going to use this as evidence

in their case to show that Yael is a bad mother. Grace has posted some of these videos on Facebook and Yael is starting to feel afraid of Grace.

Digital Evidence Collection

Grace could potentially be charged with the criminal offence of harassment. Yael may also be able to sue Grace for breaching her privacy, defaming her, or intentionally inflicting mental distress. Because they are already involved in a family law dispute, Yael could seek a protection order limiting Grace's contact with her and/or her son. As Grace is afraid for her safety, she might also decide to go to the police and ask for a peace bond. For information about the processes for obtaining peace bonds and protection orders, see: Peace Bonds and Protection Orders for Victims of Technology-Facilitated Violence. For detailed information about possible legal remedies in cases of technology-facilitated stalking and harassment, like the scenario set out above, see Legal Remedies for Online Stalking, Harassment, Spying, and Threats.

To support any complaints to the police or a civil claim, Yael will need to collect digital evidence of Grace's harmful behaviour. Throughout, Yael should be mindful of any risks to her safety that might result from collecting this evidence. See: Safety Considerations for Preserving Digital Evidence.

Below is some general information about the types of evidence Yael should try to preserve. For more information, see Preserving and Storing Evidence of Technology-Facilitated Violence: Best Practices and the guides on preserving certain types of digital evidence linked below.

Text Messages

- Yael will want to keep a copy of all the text messages Grace has sent her to show how excessive the texting has been. In a case like this, it could be thousands of messages, which means it would be very time-consuming to screenshot each one. She can see if the messaging application she uses has the option to export all of the texts at once. Otherwise, she can screen record or take a video of her slowly scrolling through all the text messages, and then screenshot the texts that are relevant to her case according to the advice of the police or her lawyer.
- She should make a note of and screenshot any date and time when Grace sent messages that were harassing, threatening, excessive, or made Yael uncomfortable. The court may or may not want to read every single message Grace ever sent, so it is important to have all the messages saved while also working with a lawyer or police to identify which specific messages are relevant. Once Yael or her lawyer has determined which are relevant to her case, she can then show the court those texts.
- She should make a note of and screenshot any date and time when she sent a message to Grace asking her to stop sending so many messages or saying that she was making Yael uncomfortable.

Email Messages

- Yael will want to keep a record of all of the emails that Grace has sent her.
- She should keep the original copy of all of the emails. These emails contain important metadata about when the email was sent and from whom. If the email is forwarded and then saved, it loses the metadata from the original message.
- She may want to create a special folder in her email account where she stores all of the emails from Grace. Because Yael is worried Grace has access to her email account, she should make sure to save additional copies of these emails on her hard drive, on a USB drive, or elsewhere. If Grace has access to Yael's email account, she may delete

the messages. Yael should also consider changing the password to her email account and any other accounts Grace may have access to, if it is safe to do so.

- If she prints out the emails, she should print out all the messages that go back and forth on an email chain in one document. This will make it easier for the court to follow, compared to printing out each email and response individually.

- She should keep a second document, such as an Excel spreadsheet or a Word document, that makes notes of which emails contain what information and to make note of any emails that were harassing or threatening.
- Yael should also make note of any emails that she sent to Grace to tell her to stop sending so much communication or that it was making her uncomfortable.

Evidence of Unauthorized Access to Email

- Yael should go into her email account and look at the "Last Account Activity" or "Account Activity" to see if any unusual IP addresses are accessing the account. Yael will need to know her own IP address and will need to remember if she has used other Internet connections, such as her workplace or a coffee shop, to cross-reference the IP addresses listed on the account.
- If there are unidentifiable IP addresses, Yael should take a screenshot of them as it might help show that Grace has been accessing her email if one of the IP addresses that accessed her account is Grace's. However, if Yael doesn't know what Grace's IP address is, it may be difficult to find out. Yael may need to get assistance from the police or the court to do this. Yael will need to bring evidence of why she thinks Grace is accessing her emails, such as any of the texts or emails that mentioned things that Grace could only know if she had access to Yael's email.

Evidence of Facebook Messages

- If Yael is friends with Grace on Facebook and can see the posts herself, she should take screenshots of the posts that Grace makes about Yael, including the posts of the videos Grace has filmed of Yael and their son.
- She should make sure the screenshot includes the date and time of the post and information that can prove the account belongs to Grace. The evidence will need to show a connection between Grace and the posts.
- She should take a screenshot of the profile information associated with the account. If Grace uses a fake name on her profile, it will be important to collect other evidence shows that Grace uses that account, such as other posts on the account that have her photo or other information that could prove it is her account.
- If Yael is not friends with Grace on Facebook, she may need to ask a friend or family member to collect this evidence on her behalf. She may need to ask that friend to act as a witness if the case goes to court.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you or call/text the Kids Help Phone to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

We gratefully acknowledge Moira Aikenhead for providing expertise to update this toolkit and Suzie Dunn of The eQuality Project at the University of Ottawa for providing expertise and guidance on the creation of this information sheet.

Adapted with permission from BCSTH's Technology Safety project, based on their resource Technology-Facilitated Violence: Preserving Digital Evidence Toolkit.

This document is part of a series of resources provided through Women's Shelters Canada's Tech Safety Canada project. We encourage you to visit www.techsafety.ca to find additional information and resources about technology-facilitated violence, technology safety planning, and preserving digital evidence. This document, or any portion thereof, may be reproduced or used as long as acknowledgement is included. If you would like to adapt the content, please contact Women's Shelters Canada at info@endvaw.ca.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada | Femmes et Égalité des genres Canada | Canada