Considerations Before 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.

An Introduction to the Preserving Digital Evidence Toolkit

When experiencing technology-facilitated gender-based violence (TFGBV), it is important to document and save digital evidence as soon as possible in order to preserve it, whether or not you intend to take legal action. Preserving evidence means it is available later if you do decide to take legal action.

TFGBV is when technology (such as a smartphone, computer, Smartwatch, or a Smart home device) is misused to commit violent abusive acts such as domestic violence, harassment, stalking, sexual assault, impersonation, extortion, and the non-consensual filming and sharing of intimate images.

Digital evidence of TFGBV, and other forms of gender-based violence, can include photographs, video recordings, emails, and text messages.

This toolkit focuses on when and how to preserve digital evidence of TFGBV. You can find more information about what laws might apply to your particular circumstances of TFGBV in the Legal Remedies Toolkit. See, for example, Legal Remedies for Image-Based Sexual Abuse and Legal Remedies for Online Stalking, Harassment, Spying, and Threats.

Technology Isn't the Problem

Technology is not the problem. Violence against women is the core issue at the heart of TFGBV. Technology misuse is one tactic among many that perpetrators use against women and gender-diverse people, and this type of violence is usually not isolated. If technology were removed from a violent relationship, the abuse would likely continue in other forms. Women cannot control or predict the violence they will experience, nor are they responsible for the actions of their abuser. Technology simply extends the reach of the perpetrator, and it can change the form and frequency of violence for women.

Women's Right to Technology

It is unrealistic to tell women to stop using technology to avoid violence. Women should not have to get rid of their devices, stop using social media, go offline, or ignore harassing texts or emails as solutions to end TFGBV. Technology has become a necessity in our everyday lives, and it can serve as an important lifeline for women in an emergency and for accessing their support network. Women may need to remain online for their job or school, to stay connected to family and friends, or to contact help in case of an emergency. In some cases, women may even be mandated to communicate with their perpetrator as part of a court order when they have children together.

For some women, going offline may escalate the risk of violence if their abusers then seek them out in person.

In no way should women's experiences of technology-facilitated harassment, threats, and stalking be minimized because the violence happens online. Making a distinction between someone's online life and offline life is a flawed understanding of the reality of the modern world. A woman's offline life is inseparable from her online life and negative experiences online will affect woman's offline. Women's experiences of violence, whether online or in person, must be taken seriously.

Prioritizing Safety

Before preserving and storing digital evidence, you need to consider potential safety risks. There are many ways perpetrators can monitor your online and digital activities. If a perpetrator is monitoring your devices or accounts, they may be alerted to the fact that you are collecting and preserving evidence. This can put you at risk of escalated violence or lead to the destruction of digital evidence by the perpetrator.

With the support of an anti-violence worker, you should consider what technology the perpetrator still has access to (e.g. through physical access to your devices, access via cloud storage, knowing your passwords to online accounts and services, or through invasive stalkerware) before preserving digital evidence or deciding where to store that evidence. By developing a safety plan, you can identify any potential safety risks and strategize the safest ways to preserve and store digital evidence. A list of Technology Safety and Victim/Survivor Resources is available in this toolkit. You should also consult Safety Considerations for Preserving Digital Evidence before preserving digital evidence.

Digital Evidence

Even if you decide not to take legal action, you may want to keep evidence of abuse to show your friends, family, victim service worker, or another support person.

If you choose to pursue legal action, it is important to collect digital evidence as soon as possible. With many apps and digital devices, it is easy for this type of evidence to be deleted, lost, or manipulated, so making copies and backups right away can help ensure the evidence is preserved.

Digital evidence is an overarching term that includes: information stored on electronic devices (e.g.. phones, tablets, computers), text messages, direct messages (DMs), pictures, videos, voice recordings, screenshots, account logs or billing statements, apps, location information, or metadata (i.e. the information embedded in electronic documents such as emails, photos, or screenshots), among other things. It is worth noting that under the *Canada Evidence Act*, all forms of digital evidence are referred to as "electronic documents."[1] Within this toolkit, we will use the term "digital evidence" rather than "electronic documents."

The information within this toolkit is not legal advice. Rather, it provides general legal information about digital evidence and technology-facilitated violence. The information for preserving evidence within this toolkit does not replace the evidence collection rules, policies, and protocols of law enforcement or the legal system. Instead, this toolkit aims to provide practical information for survivors to help preserve evidence for safekeeping, or to pursue criminal or civil legal action. Survivors involved in criminal, civil, or family law cases are encouraged to contact legal advocates in their community to access legal supports and to receive current legal advice from a licenced lawyer. If you wish to pursue a legal remedy, please consult Legal and Victim Service Supports and Resources.

The Preserving Digital Evidence Toolkit helps women and frontline anti-violence workers:

- understand the benefits of preserving and storing evidence of TFGBV;
- consider the most effective ways of preserving and storing evidence of TFGBV;
- identify what digital evidence is relevant to civil or criminal cases of violence against women, including the technologies that are used to perpetrate TFGBV;
- understand some of the legal rules of digital evidence and related resources; and
- give practical suggestions on how to preserve and store digital evidence.

Before reviewing the resources within the toolkit, several important considerations serve as a starting point.

The Digital Trail of Evidence

While experiencing TFGBV, some survivors will be aware of the technology the perpetrator is abusing. They may know that the perpetrator has the passwords to their phone or social media accounts, is using a program to track their location, has access to an intimate image, or is posting harmful messages about them online. Others may only know that the perpetrator knows too much about their conversations, whereabouts, or activities. In such cases, survivors may only suspect the perpetrator has access to their device, accounts, or location via technology. Others may not be able to identify the person who is harming them.

With TFGBV, there is almost always evidence of the violence, such as threatening text messages or an IP address linked to unauthorized access to an email address. Digital evidence may also be found in more than one place such as on a smartphone, social media platform, and within the servers of a social media company. It is important to consider all possibilities of where digital evidence could be stored. **Making a list of the types of technology (e.g. devices, apps, and online accounts) you use, and considering whether or how the perpetrator is using that technology to harm you, can help determine what technology is being misused.**

Speaking with an anti-violence worker who understands technology-facilitated violence can help you determine what type of evidence you should be looking for. The questions anti-violence workers ask during a safety planning session can help narrow down what form of technology is being misused.

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 Technology-Facilitated Violence: Preserving Digital Evidence Toolkit.

---

1. Under s 31.8 of the *Canada Evidence Act,* "electronic document" is defined 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, printout or other output of that data." ↥

Safety Considerations for Preserving Digital Evidence

This first section of this document focuses on safety considerations for survivors **before** taking steps to preserve digital evidence. Please read this section before you begin collecting digital evidence. There are unique risks involved in saving digital evidence that you should take into consideration in cases of technology-facilitated gender-based violence (TFGBV) or other forms of violence and abuse. This handout discusses the importance of making a safety plan around evidence collection, which can help you avoid further abuse and can help save evidence from being lost.

Women experiencing TFGBV often have access to large amounts of evidence of that violence, which may include:

1. **Evidence that you have direct access to,** such as evidence on your digital devices and evidence that can be accessed through your online accounts. It is not uncommon for a perpetrator to send dozens, if not hundreds, of unwanted texts and emails. You may likely have received (and saved) abusive messages and other proof of violence from a perpetrator that can be useful to prove that you are experiencing violence. Sometimes you will automatically have a copy (e.g. if your abuser sends an abusive email, you will

automatically have a copy of it in your email folder). Other times, you have to find a way to save it yourself; for example, if your abuser posts a threat to you on his social media account, you will need to take a screenshot.

2. **Evidence that you do not have direct access to**, such as information on the accounts of, or messaging apps of, friends of the perpetrator. For example, if your abuser has shared a nude image to a private messaging group of which you are not a member, you may need to gain access to the image through someone else.
3. **Evidence that perpetrators have access to**, which may be shared with you (such as on a shared account). Sometimes, only the perpetrator will have access to this.
4. **Evidence that you may need technical support to gather**, such as determining if stalkerware has been installed on your phone.
5. **Evidence that needs to be obtained by court order or subpoena.** This might include evidence from third parties such as information from Internet Service Providers, telecommunications companies, or websites. For example, there may also be evidence on devices and online accounts that can help show what kind of violence you are facing and the identity of the perpetrator, such as evidence showing which IP address or device accessed the account recently.

For an overview of the types of behaviours that may result in digital evidence, and what sorts of evidence you may want to collect in these scenarios, see: Preserving Digital Evidence Example: Sexual Images Shared Online and Preserving Digital Evidence Example: Online Harassment.

Consider Risks to Safety

Perpetrators committing TFGBV will often monitor women's accounts and devices as a way to exert power and control and extend their abusive behaviour. Before preserving digital evidence, it is important to consider any risks to your safety and the risks of losing important evidence.

If the perpetrator is alerted that evidence is being collected (e.g. if they are monitoring your behaviour or have access to your devices), there may be a risk of violence escalating or critical evidence being deleted. For example, a perpetrator may have access to your cloud storage account and see that screenshots, photos, videos, and conversations are being preserved and backed up to the cloud.

Connecting with a local Victim Service Worker or anti-violence program to assess the potential risks and develop a technology safety plan can help you safely strategize ways to preserve digital evidence. For example, anti-violence workers can help determine alternative ways to preserve evidence if you think that your abuser may become more violent if they learn that steps have been taken to preserve digital evidence. Anti-violence workers can help strategize how to collect evidence without alerting the abuser, and ways to effectively save (and back up) evidence. For a list of anti-violence resources, see Technology Safety and Victim/Survivor Resources.

Posting Digital Evidence Online

Some women have posted digital evidence (photos or videos) of the violence they experienced online. Understandably, you may want to share your experience of abuse with your social network. However, this step should be pursued cautiously. Posting evidence online could alert an abuser that you are taking action against the violence you have experienced. This may give that person the chance to destroy incriminating evidence about the violence. This in turn could prevent law enforcement from collecting the evidence needed for criminal investigations. It is also important to note that, in some court cases, judges have negatively viewed victims' posting of digital evidence on social media or the Internet.

Storing Digital Evidence

Storing Digital Evidence on a Device

You can store digital evidence directly on your digital devices, such as your phone, computer, or laptop, if you believe they are secure. However, if the perpetrator lives in the same home as you or can access these devices, there is a risk that they could discover this evidence. You may want to ask a trusted friend to store this evidence on one of their devices instead. You could also save this evidence in an account or in an application that the perpetrator does not have access to. If you cannot safely keep the evidence on your device, transfer it elsewhere and delete the file from the device. Once deleted, remove any "recycle bin" copies made. Some devices like Apple iOS store deleted photos and videos in a "Recently Deleted" album for 30 days, or until removed from the device. Ensuring the photos and videos are deleted from all spots on the phone can be an important part of a safety plan.

> ***#TechSafetyTip*** Only save evidence of violence on your devices if the perpetrator does not have physical or remote access to these devices.

Because there is always a risk of an account getting corrupted or a device getting lost or destroyed, you should back up the evidence on a second account or device and, if possible, keep a printed hard copy for your records. It is not uncommon for a computer to crash or a phone to get damaged. Backing up the digital evidence on a second account minimizes the risk of loss.

> ***#TechSafetyTip:*** Ensure you have copies saved elsewhere than on your device, such as with a friend, or using an external storage option.

If you know or suspect that the perpetrator has the passwords to your accounts, change all of your passwords immediately to ones that the perpetrator cannot 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 that can be turned off in the settings. This can prevent your abuser from gaining access to and removing or tampering with your evidence.

> ***#TechSafetyTip*** Create new accounts or change the passwords to any existing accounts where you are storing digital evidence of abuse.

Perpetrators may be monitoring your accounts using mobile spyware. If they are monitoring your devices in this way, it may alert them to the fact you are collecting digital evidence or allow them to delete the evidence. If you have any concerns that your device(s) may be infected with spyware, plan how to change passwords to your accounts on a device the perpetrator does not have access to so that the perpetrator is not alerted.

#TechSafetyTip Look at your account settings to see what devices are connected to the account and disconnect unknown devices or the perpetrator's devices from the account if it is safe to do so.

External Storage Options

Storing digital evidence on an external storage device like a USB memory stick is a good option. To transfer files off of your cellphone and onto a storage device, you may first need to transfer them to a computer where you can attach your USB. Make sure you are using a secure device that the perpetrator does not have access to. Check your device for what is needed to transfer files from your smartphone to an external hard drive or USB memory stick, and if it is possible for the model of your smartphone. iPhones, for example, may need specific apps and adapters to transfer files to a USB memory stick. Most Android devices require the same connectors as your phone.

Note that if you are planning to rely on the file as evidence in a legal proceeding, **it is best to move it as few times as possible to minimize questions about its authenticity**. Keep a record of the steps you took to record and transfer all digital evidence, every time you transfer it, email it, or save it to a new device.

Cloud Storage

Storing digital evidence in the Cloud using an online storage solution like Dropbox, Google Drive, iCloud, or others can be a great option if having a physically saved copy is a safety risk. This option can also be simpler than external storage options and may remove the need to purchase any other devices or adapters.

Many cloud storage providers offer free trial plans that are limited in storage. Despite being limited in size, in most cases, these services offer enough storage for a fair amount of screen recordings.

Some example services are:

- Dropbox
- Google Drive
- Amazon
- PCloud
- iCloud

The following are cloud storage safety planning considerations:

- Do not download a video screen recording app for your cloud storage provider that connects directly to your account and/or indicates you have used such an app. The exception would be if you normally use the app for other personal reasons, such as using one for work purposes. You may want to turn off the function of automatic downloading.

  #TechSafetyTip If you are using a cloud storage app for personal reasons, create a different account when uploading digital evidence. This will help keep you organized and may protect you from the perpetrator accessing the files if they have access to or knowledge of your personal account.

- If you think the perpetrator may be monitoring your email, you should sign up for cloud services with a new or existing email account that the perpetrator does not have access to. For example, if you use a shared email account with the perpetrator or if they know your email password, the perpetrator can use a password reset on the cloud storage account to gain access to it. Updates from your cloud storage provider likely will be communicated via email and can signal to the perpetrator that you have an account.

  #TechSafetyTip Sign up for any new cloud services with an email that the perpetrator does not have access to.

- Create a new email specifically for uploading your digital evidence to the Cloud. There are a lot of free email account services, such as those listed below. As a bonus, some email providers also offer free limited cloud storage.
  - Mail.com
  - Gmail.com
  - Outlook.com
  - Protonmail.com

- Be cautious when accessing an email or cloud storage website with a web browser. By default, web browsers keep a browsing history, which the perpetrator may access if he has access to your device or to browsers that store history across devices, such as Google Chrome.

  #TechSafetyTip Delete your browser history after visiting any sites where you are storing your video screen recordings.

- When apps are downloaded from an app store, the history of what apps you have currently and previously installed will often be listed in your app store account.

  #TechSafetyTip Consider using a web-based cloud storage solution rather than an app on your phone or computer.

- Typically, most online storage options are based in the United States and are therefore bound by US law. Despite how private you may think your cloud storage account is, there is also a possibility that US law enforcement sources may have access to it. Generally, this poses a low risk to users, but should still be considered.

Decoy Apps

In many app stores, there are apps commonly referred to as "decoy apps." These are file storage apps designed to avoid suspicion by pretending to be different apps.

A common example is a calculator decoy app. This app works exactly like a traditional calculator. But, type in a special code like "36x%29=" and it will open a file folder within the app to save pictures or videos.

It is important to note that even if you are using a decoy app, the files are still stored on the device, although they are hidden at first glance. There are ways perpetrators could determine if a device contains a decoy app, such as if the perpetrator is familiar with these apps or is monitoring your device using stalkerware. For more information about

stalkerware, see WSC's information on Mobile Spyware.

Connect to an Anti-Violence Worker or Legal Advocate for Support

If you are unsure how to preserve evidence of technology-facilitated violence, contact an anti-violence program in your area for support and to develop a safety plan that includes technology safety considerations. See Technology Safety and Victim/Survivor Resources.

Collecting Digital Evidence

There are a variety of ways to preserve digital evidence of online abuse. How you preserve this evidence will depend on what type of evidence it is, what you are hoping to prove, where it is stored, and any potential risks to your safety. See Preserving and Storing Evidence of Technology-Facilitated Violence: Best Practices for a general overview and the guides on screen recording, screenshots, video recordings, audio recordings, websites, and emails for specific tips and methods.

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 Safety Considerations for Women Preserving Digital Evidence. Adapted for Canada with permission from NNEDV's Safety Net project, based on their Legal Systems Toolkit.

---

1. Under s 31.8 of the *Canada Evidence Act,* "electronic document" is defined 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, printout or other output of that data." ↥

Preserving Digital Evidence: Considerations for Anti-Violence Workers

Anti-violence workers are a valued source of support for women and gender-diverse people experiencing technology-facilitated gender-based violence (TFGBV). An anti-violence worker can follow the steps below to assist in strategizing a technology safety plan for a woman facing technology-facilitated gender-based violence.

Step 1: Work with Survivors to Identify All Technology Misused

When meeting with a woman experiencing violence, it is important to discuss:

- How technology played a role in the abusive relationship, including all communication methods, devices, and programs used by the woman in her daily life, particularly those used to communicate with the perpetrator
- If and how perpetrators have access to technological devices or accounts (either physical or with digital access)
- Whether there was any technology-related violence in their relationship, and what the abusive behaviour was (e.g. threats, harassment, monitoring, sharing intimate images)
- Whether the woman suspects that the perpetrator may be accessing her devices, digital accounts, or location secretly or without consent
- Whether there is any digital or electronic information that the perpetrator has access to that may pose a safety or communication risk
- If there is any evidence of the abuse or violence that is at risk of being lost or deleted
- The possible locations where the digital evidence of the technology-facilitated violence can be found

For more information on safety planning with victims of TFGBV, see BCSTH's Assessing for Technology- Facilitated Violence and Privacy Concerns for Anti-Violence Workers.

Step 2: Protect the Data

Once the technological devices and accounts that have been or are being misused are identified, you can begin the process of locating the digital evidence. It can be useful to make a list of the evidence that may still need to be collected and what has already been collected.

It is important to determine where the digital evidence is currently stored (e.g. in a text message on the woman's phone, in an email on her email account, on a social media page, or on her iCloud account) and to consider how to protect or freeze the data before actually preserving the digital evidence. This could include blocking the perpetrator's access to accounts. To block unwanted access to their personal accounts, women can change the passwords on all relevant platforms and devices. It is important to be aware that if an account becomes blocked, this can lead to the automatic deletion or inability to access digital evidence.

A safety assessment should be done before making any changes to an account's privacy settings, password, follower/friend list, or saved data. Changes such as these may alert the perpetrator that the woman is collecting evidence or seeking help. This can lead to an escalation in violence and/or the deletion of evidence by the perpetrator. Making a safety and evidence preservation plan, before taking any action, is important for the safety of the woman and the strength of any future legal case she may choose to pursue.

Cloud-Based Accounts

Changing passwords and device access is particularly important for cloud-based accounts such as iCloud or Google Drive. These accounts are commonly connected to many devices (e.g. phones operating on the same system, tablets, laptops, desktop computers, and fitness accessories) and will automatically sync information and back up data across

several devices. Perpetrators may have access to cloud-based accounts by either knowing the password or having access to a device that has been set up with the cloud account information on it so that a password is not required for access. Women should identify what cloud-based accounts are linked to their device(s) and, if possible, which accounts perpetrators have access to. This could include devices that aren't commonly thought of, such as the perpetrator's smartwatch, Bluetooth-connected speaker, or smart car. Remote access to cloud-based accounts may allow perpetrators to see what evidence is being preserved. Having remote access to cloud accounts also gives perpetrators access to destroy any evidence that is stored there.

Stalkerware

Stalkerware is a broad category of malware that allows a perpetrator to monitor a woman's phone activity and/or track the location of her phone. For more information about stalkerware, see WSC's information on Mobile Spyware. If there are concerns that a device is infected with stalkerware, it is important to create a plan for how to change passwords without alerting the perpetrator, who may have access to the device's activities (e.g. not creating a new password on the device that is being monitored, as the perpetrator may have been monitoring the change and will then know the new password as well). Once a plan to avoid detection is created, women and anti-violence workers can create strong passwords that are unlikely to be breached.

Automatic Deletion

Digital evidence can also be lost through normal device and account functioning. To increase the speed and usability of devices, many companies set up devices and accounts to automatically delete information. Devices or accounts should be reviewed to determine if they are set up to automatically delete messages after a certain amount of time. If the device is programmed this way, account settings can be changed to stop automatic deletion and allow for digital evidence to remain stored on the device.

Backup

It is important to have a secondary backup of all digital evidence. Digital evidence can be compromised or made unavailable if a device is lost, stolen, or broken. A secondary backup can be another device or account, printed physical copies of the evidence, or both. As accidents happen, plan early for how to back up evidence.

Step 3: Explain Limits to Anti-Violence Worker's Involvement in Preserving Evidence

Many women being supported by anti-violence workers ask them to take photos and make recordings of TFGBV as a means to preserve evidence. They may also be asked to store copies of digital evidence securely. However, by personally assisting in digital evidence preservation, it may open up the risk that an anti-violence worker or their client's file will be subpoenaed by the court to explain how and why they collected the evidence. This could potentially lead to them being questioned, by opposing counsel or the Crown, about their work supporting women and their families. Additionally, if the photographic or digital evidence is stored in women's case files and is commingled with other records, such as notes of her meetings with anti-violence workers, those records may open the woman's entire support file to discovery as well. In this situation, perpetrators, along with opposing counsel or Crown, may subpoena the organization's records to gain access to copies of the evidence.

Anti-violence workers can work with women to discuss the possible consequences of having a third party, such as themselves, preserve evidence. An integral part of technology safety planning is identifying which methods of digital evidence preservation are in the best interests of the woman in the long run. In some circumstances, it may be appropriate or necessary for anti-violence workers to collect or store evidence, but it is important to discuss the risks with the client before doing so. Clients should be encouraged to collect evidence themselves, or have a family member or friend collect that data for them, whenever possible.

Many anti-violence programs have a records management policy of only recording the minimum amount of information necessary to provide the services needed for the time required. Check with your organization's policies, and if there is no policy, advise your organization that it should consider writing one.

Step 4: Discuss How to Document the Evidence

It is common for women to collect and preserve evidence themselves by saving emails, recording messages, taking screenshots, or printing evidence. As part of technology safety planning, anti-violence workers can provide women with resources that explain what information is important to retain, and how to document experiences of technology-facilitated violence as effectively as possible. Guidance can be provided as to the necessary steps to preserve the evidence in a format that will be considered authentic and complete. Doing so will minimize opportunities that might negatively impact the collection process.

Encouraging women to back up their evidence in multiple places is also suggested, as long as this can be done safely.

Documenting digital evidence in chronological order is best. Women's Shelters Canada has created a Technology-Facilitated Violence Log that you can use to help women keep a record of their experiences of technology-facilitated violence.

Technology is always evolving and it can be challenging for anti-violence workers to learn about and stay up to date on technology and digital evidence preservation. Many anti-violence workers may be unfamiliar with what technologies exist, how the technology can be used to perpetuate violence, and how to collect digital evidence. It may be useful to read the additional documents in this Toolkit to gain information about the technologies and techniques that can help your clients.

Step 5: Refer Her to a Legal Advocate or Lawyer

Women may need additional legal information or advice about how to preserve digital evidence and relevant legal remedies. To find organizations in your province or territory that provide legal information, legal aid, or legal assistance see: Legal and Victim Service Supports and Resources.

Step 6: Provide Additional Technology Safety Resources

For additional resources for you and the people you are assisting, see Technology Safety and Victim/Survivor Resources.

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.

Adapted with permission from BCSTH's Technology Safety project, based on their resource Preserving Digital Evidence: Considerations for Anti-Violence Workers Supporting Women.

---

1. Under s 31.8 of the *Canada Evidence Act,* "electronic document" is defined 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, printout or other output of that data." ⤴

Technology Safety and Victim/Survivor Resources

This document provides links to resources that may be helpful if you are experiencing or know someone who is experiencing technology-facilitated gender-based violence (TFGBV). It includes links to information about technology-facilitated violence, as well as support resources for victims/survivors of this violence across Canada.

These resources are based outside of the legal system and will not necessarily involve engagement with the legal system or any legal advice. If you are interested in pursuing legal remedies in response to technology-facilitated violence, such as making a claim in civil or family law or pursuing criminal charges, you should consult the Legal Remedies Toolkit. In particular, if you are interested in information and support concerning a legal remedy such as Victim Services or Legal Aid, see Legal Supports and Resources.

French-language resources are available here

National Resources

Online Safety Guides and Resources

- Online Safety Guides and tip sheets created by the Edmonton Police Service
- Cybertip.ca This website, operated by the Canadian Centre for Child Protection, provides age-appropriate information and resources to help educate Canadians about how to keep children safe while online and reduce child victimization. It includes information about intimate images, sextortion, and other online safety resources.
- Canadian Anti-Fraud Centre This website provides information about past and current online scams impacting Canadians.
- Online Safety Resources This website of the Canadian Centre for Child Protection includes links to online safety resources for children and youth.
- The Citizen Lab – Tools and Resources These resources contain information about protecting your information and privacy online. Created by the CitizenLab at the University of Toronto.
- DontGetSextorted.ca - This website provides information and techniques on avoiding sextortion online.
- A Guide for Trusted Adults This resource by Media Smarts is designed to prepare parents, guardians, teachers, and mentors to assist young women when they face problems online.
- Tech Without Violence This resource, created by the Ottawa Coalition to End Violence Against Women, contains prevention information and guides relating to cyberviolence and online safety.
- A Quick Guide on Sexual Image-Based Abuse. This guide created by YWCA Canada outlines rights, resources, and supports about sexual image-based abuse.

National Helplines

- Assaulted Women's Helpline This helpline is available 24 hours a day, 7 days a week, in over 200 languages, including 17 Indigenous languages. Based in Ontario.
- Kids Help Phone 24-hour online and phone counselling available for those 5-20 years old.
- Hope for Wellness Helpline This support helpline is available 24/7 for Indigenous people across Canada.
- Youthspace. Online youth crisis and emotional support text and chat service, available 6 p.m. to midnight PST.

Domestic Violence Shelters and Services

- Sheltersafe.ca provides an interactive map of shelters for victims of domestic violence across Canada.
- Ending Violence Association of Canada maintains a list of shelters, transition houses, and support services available across Canada.
- Family Violence Responses This list of federal laws and programs related to family violence was compiled by the Government of Canada.

Sexual Assault Centres, Crisis Lines, and Support Services

- The Ending Violence Association of Canada maintains a list of national and province/territory-specific sexual assault centres, crisis lines, and support services.
- Draw-The-Line.ca is an online resource containing tools and information for preventing and addressing sexual violence, including certain forms of online violence. Based in Ontario.
- Technology Safety Canada Project Resources The resources on this website by Women's Shelters Canada contain information about technology safety, technology-facilitated teen dating violence, and other useful information.
- Unacceptable This guide, created by the Women's Legal Education and Action Fund, contains information about the forms of technology-facilitated violence and options and remedies for victims of this violence.
- GetCyberSafe.ca This website, created and maintained by the Government of Canada, contains information and resources on securing your digital devices and online accounts.
- Stay Safe Online Guide created by the Government of Yukon.

International Resources

Online Safety Guides and Resources

- Safety Net Project The National Network to End Domestic Violence has developed technology safety toolkits including a survivor toolkit and an app safety toolkit. Based in the United States.
- Combatting Cyber Sexual Abuse: A Manual for Advocates This manual prepared by the New York Cyber Sexual Abuse Task Force is designed to assist those advocating for and working with survivors of online sexual violence. Part 6 includes a section on technology safety planning and best practices. Based in the United States.
- Deepfakes: A Victim Resource Guide This guide compiled by EndTAB includes resources, tools, and strategies for anyone who has had deepfake videos created of them. Based in the United States.
- CCRI Safety Center The Cyber Civil Rights Initiative has created an online Safety Center with information and resources for victims of technology-facilitated violence. Based in the United States.
- Women's Technology Safety and Privacy Toolkit This toolkit by Technology Safety Australia provides a large volume of information and resources about online privacy and safety. Updated frequently. Based in Australia.
- App Safety Centre This website by Technology Safety Australia contains information reviewing various personal safety apps. Based in Australia.
- DIY Cybersecurity for Domestic Violence This website created by HACK*BLOSSOM contains resources and strategies for victims of technology-facilitated abuse by their intimate partner. Based in the United States.
- Clinic to End Tech Abuse – Resources This website contains how-to guides related to online privacy and technology-facilitated violence. Based in the United States.
- Crash Override Resource Centre This website contains tools, guides, and educational materials related to online privacy. Based in the United States.
- Online Harassment Resources This resource by HeartMob provides information and guides related to technology-facilitated violence and online safety. Based in the United States.
- Extreme Privacy This resource contains a list of companies offering online information removal services. Based in the United States.
- Stalkerware Detection, Removal, and Prevention This resource provides information about stalkerware and removing it from your device. Based in the United States.
- Speak Up & Stay Safe(r) This guide, produced by Feminist Frequency, contains information for preventing and addressing doxxing and online harassment. Based in the United States.
- Consumer Reports Security Planner This online tool creates a personalized plan for securing your data. Based in the United States.
- Surveillance Self-Defense This resource created by the Electronic Frontier Foundation contains guides for protecting yourself online. Based in the United States.
- Digital Rights and Privacy Resources This list, compiled by Best VPN, contains links to mobile privacy apps, computer privacy software, and other resources. Based in the United States.
- eSafety Commissioner Australia This website contains information and resources on maintaining safety and privacy online. Based in Australia.
- Resources – Hacking//Hustling This website contains online safety resources and technology safety tips. Based in the United States.
- Cyberbullying This resource, created by the Office of Children and Family Services of New York State, contains courses on cyberbullying and sexting tailored to users 14 and under as well as 15 and over. Based in the United States.
- Nonconsensual Pornography (NCP) This toolkit created by Operation Safe Escape explores issues around nonconsensual pornography. Based in the United States.
- Stalkerware This toolkit created by Operation Safe Escape explores issues around stalkerware. Based in the United States.
- PEN America Online Harassment Field Manual This website provides tips and resources for responding to online harassment.
- The Data Detox Kit This toolkit, created by Tactical Tech, includes steps you can take to secure your privacy and secure your online life.
- Take Back the Tech This website contains resources and information on gender-based violence taking place online including extortion and harassment.
- Digital Hygiene Lessons This resource prepared by TrollBusters includes tips for managing your data online.

Yukon

Domestic Violence Shelters and Services

- Family Violence Responses – Yukon This list of laws and programs in the territory related to family violence was compiled by the Government of Canada.
- The Victoria Faulkner Women's Centre Provides a safe space for women to connect and access support services.
- List of Women's Shelters This list and contact information is maintained by the government of Yukon.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Get Help: You Were Sexually Assaulted This list of information and resources is maintained by the Government of Yukon.

Northwest Territories

Domestic Violence Shelters and Services

- Family Violence Responses – Northwest Territories This list of laws and programs in the province related to family violence was compiled by the Government of Canada
- Family Violence Service Contacts and Information This list is compiled by the Status of Women Council of the Northwest Territories.
- NWT Family Violence Shelters This list of shelters and contact information is maintained by the government of the Northwest Territories.
- NWT Community Counselling Program This program provides access to counselling and mental health services across the Northwest Territories.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.

- Sexual Violence is Never OK This list of information and resources related to sexual violence is maintained by the Status of Women Council of the Northwest Territories.

Nunavut

Domestic Violence Shelters and Services

- Family Violence Responses – Nunavut This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Cambridge Bay Wellness Centre Provides a variety of wellness programs including counselling and support services.
- Family Violence Shelters This list of phone numbers for Nunavut shelters is maintained by the Government of Nunavut.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Believe-Ask-Connect This online collection of resources for individuals experiencing violence is maintained by Pauktuutit Inuit Women of Canada.

British Columbia

Domestic Violence Shelters and Services

- Family Violence Responses – British Columbia This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Technology Safety Project Resources – BC Society of Transition Houses The resources on this website contain information about technology safety, technology-facilitated teen dating violence, and other useful information. See also Technology Safety and Privacy Toolkit.
- VictimLink BC This service provides information and referrals to all victims of crime and immediate crisis support to victims of family and sexual violence.
- "Need Help" – List of Services from EVA BC – The Ending Violence Association of BC maintains a list of domestic violence supports across B.C., divided by region.
- BCSTH Directory of Programs and Services The BC Society of Transition Houses maintains a list of transition houses, safe homes, and other programs and services across BC related to domestic violence.
- Women Fleeing Violence This list of transition houses and other housing and support programs is maintained by BC Housing
- Community Resources for Metro Vancouver This list of family violence resources is maintained by the Vancouver and Lower Mainland Multicultural Family Support Services Society.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- VictimLink BC This service provides information and referrals to all victims of crime and immediate crisis support to victims of family and sexual violence.

Alberta

Domestic Violence Shelters and Services

- Family Violence Responses – Alberta This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- ACWS Member Shelters This map of shelters across Alberta and contact information is maintained by the Alberta Council of Women's Shelters
- Find Shelters This list of family violence shelters and other housing initiatives is maintained by the Government of Alberta.
- Find Your Program This list of community service programs is maintained by the Family and Community Support Services Association of Alberta.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Sexual Violence – Get Help This list of resources is maintained by the Government of Alberta.

Saskatchewan

Domestic Violence Shelters and Services

- Family Violence Responses – Saskatchewan This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Interpersonal Violence and Abuse Programs This list of services is maintained by the Government of Saskatchewan.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Sexual Assault Services of Saskatchewan – Resources Locations This interactive map provides contact information for sexual assault resource centres across Saskatchewan.

Manitoba

Domestic Violence Shelters and Services

- Family Violence Responses – Manitoba This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Find a Service by Category This list of resources and services for victims of violence is maintained by Ending Violence Manitoba.
- Resources and Supports This list of resources and supports related to family violence is maintained by the Government of Manitoba.
- Find a Shelter – This list of shelters is maintained by the Manitoba Association of Women's Shelters.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Klinic Community Health Sexual Assault Crisis Line This 24/7 crisis line provides support for anyone who has experienced sexual assault.

Ontario

Domestic Violence Shelters and Services

- Family Violence Responses – Ontario This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Domestic violence information sheet Created by the Government of Ontario. Includes information on hiding your Internet activity.
- Indigenous Community Wellness Workers If you are Indigenous, you can talk to a Community Wellness Worker to get programs and services for family violence.
- Healing Lodges Indigenous victims of violence may visit a healing lodge to access residential and day programs using traditional Indigenous healing and contemporary therapeutic interventions.
- Indigenous Family Violence Healing Program Women and children experiencing violence and seeking safety can find safe residential spaces and supportive and holistic healing spaces.
- Shelters for Indigenous Women and Children Women and children experiencing violence can access a short-term residence where they can obtain counselling and other support.
- Find a Centre Near You This list of sexual assault and domestic violence treatment programs is maintained by the Ontario Network of Domestic Violence Treatment Centres.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- OCRCC – Find Support This site contains links to sexual assault centres providing free counselling and information about sexual violence across Ontario. Organized by geographic location.

Quebec

Domestic Violence Shelters and Services

- Family Violence Responses – Quebec This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- SOS Violence Conjugale Offers free, bilingual, anonymous, and confidential referral services. Available 24/7 and can provide direct access to information, support or shelter.
- Justice Quebec Provides resources for couples, families, and single people related to domestic violence, sexual violence, and family law.

Sexual Assault Centres, Crisis Lines, and Support Services

- List of Sexual Assault Centres This is a list of sexual assault centres and other resources maintained by the Regroupement Québécois des centres d'aide et de lutte contre les agressions à caractère sexuel.

Newfoundland and Labrador

Domestic Violence Shelters and Services

- Family Violence Responses – Newfoundland and Labrador This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Family Resource Centres and Satellites This list of family resource centres is maintained by the Government of Newfoundland and Labrador.
- Find a Shelter This list of shelters is maintained by the Transition House Association of Newfoundland and Labrador

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Our Services – Newfoundland Sexual Assault Crisis and Prevention Centre This sexual assault centre operates a 24-hour support and information line, in-person supports, and other services.

New Brunswick

Domestic Violence Shelters and Services

- Family Violence Responses – New Brunswick This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Support Services for Victims of Abuse This list of support services is maintained by the Government of New Brunswick
- Regional Violence Prevention Networks This list of agencies working on violence prevention initiatives across New Brunswick is maintained by the Government of New Brunswick

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Sexual Violence New Brunswick This organization provides support to sexual assault survivors in the Fredericton region.

Nova Scotia

Domestic Violence Shelters and Services

- Family Violence Responses – Nova Scotia This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Our Shelters This list of women's shelters across Nova Scotia (outside of the Halifax Regional Municipality) is maintained by the Transition House Association of Nova Scotia.
- Violence and Abuse This resource from Nova Scotia 211 allows individuals to search for domestic violence resources in their region, including domestic violence shelters.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Where to Get Help This interactive map created by the Sexual Violence Prevention & Supports Department of Community Service Nova Scotia provides contact information for sexual assault services across the province.

Prince Edward Island

Domestic Violence Shelters and Services

- Family Violence Responses – Prince Edward Island This list of laws and programs in the province related to family violence was compiled by the Government of Canada.
- Emergency Services This list of emergency resources, including emergency domestic violence shelters, is maintained by the Premier's Action Committee on Family Violence Prevention of Prince Edward Island.

Sexual Assault Centres, Crisis Lines, and Support Services

- Information and Support for Victims of Sexual Assault This list of agencies providing formal and informal counselling and support for victims of sexual assault is maintained by the Canadian Association of Sexual Assault Centres.
- Prince Edward Island Rape and Sexual Assault Centre This Centre provides support for victims of recent and historical sexual violence.

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 Suzie Dunn, PhD Candidate at the University of Ottawa for the creation of this information sheet. We gratefully acknowledge Moira Aikenhead for providing expertise to update this toolkit.

---

1. Under s 31.8 of the *Canada Evidence Act*, "electronic document" is defined 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, printout or other output of that data." ⤴

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