Safety Considerations for 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.

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.

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