An Introduction to the Preserving Digital Evidence Toolkit

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.

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." ↥

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