BC Society of Transition Houses

An Introduction to the Technology-Facilitated Violence:

Preserving Digital Evidence Toolkit

When experiencing technology-facilitated violence it is important to document and save digital evidence as soon as possible in order to preserve it, regardless of whether a woman will take legal action or not. Women[1] often possess digital evidence of technology-facilitated violence before knowing how the evidence can be used to hold perpetrators accountable or before deciding to take legal action.

For those who do decide to take legal action, it is important to think about when and how to preserve digital evidence. In some cases, a woman may be considering whether or not she will involve law enforcement to pursue criminal charges of technology-facilitated crimes. These can include crimes such as threats, criminal harassment, defamation, impersonation, coercion, extortion, the non-consensual distribution of intimate images, and voyeurism.

In other cases, she may wish to preserve evidence for safekeeping in preparation for civil proceedings, such as applying for a family law protection order, engaging in guardianship and parental responsibility agreement hearings, enforcing her rights under privacy laws, or suing the perpetrator in civil court. Even if she decides not to take legal action, she may want to keep evidence of the abuse in order to show her friends, family, victim service worker, or other support person.

If a woman chooses 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 of it right away can help ensure the evidence is preserved.

Digital evidence is the overarching term that includes: electronic devices (i.e., phones, tablets, computers), texts, direct messages (DMs), pictures, videos, voice recordings, screenshots, account logs or billing statements, apps, location information, or "metadata" (the information embedded in electronic documents such as emails, photos, or screenshots), among other things. It is worthwhile to note that under the *Canada Evidence Act*, digital evidence is referred to as "electronic documents".[2] Within the resources of this toolkit, we will use the term "digital evidence" rather than "electronic

[1] In this toolkit we will be using the term "woman", "violence against women" and she/her pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. Women and girls face higher rates of most forms of technology-facilitated violence. They also experience some of the most serious consequences as a result of this violence. However, technology-facilitated violence impacts people of all genders. We hope that all people impacted by this violence will find these documents useful.

[2] S. 31. 8: Electronic document means 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 (document électronique) https://laws-lois.justice.gc.ca/eng/acts/c-5/page-5.html

documents" as it is more commonly used by everyday people when describing evidence of technology-facilitated violence.

The information sheets within this toolkit do not give legal advice, they only provide general legal information about digital evidence and technology-facilitated violence. Women 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. 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 women to help preserve evidence for safekeeping, or to pursue criminal or civil legal action.

The Technology-Facilitated Violence Toolkit: Preserving Digital Evidence helps women and frontline anti-violence workers to:

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

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

Prioritizing Safety

Prior to preserving and safekeeping digital evidence, women must consider potential risks to their safety. As outlined in BCSTH's Technology Safety and Privacy Toolkit, there are many ways perpetrators can monitor women's online and digital activities. If a perpetrator is monitoring a woman's devices or accounts, they may be alerted to the fact that she is collecting and preserving evidence. This can put the woman at risk of escalated violence or lead to the destruction of digital evidence by the perpetrator.

With the support of an anti-violence worker, women should consider what technology the perpetrator still has access to (i.e., either through physical access to her devices, access via cloud storage, knowing her 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, women can identify any potential safety risks and strategize the safest ways to preserve and safekeep digital evidence.

For more information about technology safety planning see our guide and tip sheet.

To connect with BC anti-violence programs and legal advocates:

- VictimLink BC
- Legal Aid BC
- Rise Women's Legal Centre
- Shelter Safe Map
- BCSTH technology safety planning and A Guide for Canadian Women Experiencing Technology-Facilitated Violence: Strategies for Enhancing Safety

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 not respond to harassing texts or emails as solutions to end technology-facilitated violence. 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 her support network. Women may need to remain online for her job or school, to stay connected to family and friends, or to contact help in case of an emergency. In some cases, she may even be mandated to communicate with the perpetrator as part of a court order when they have children together.

For some women, going offline may escalate the risk of violence if her abuser then seeks her 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 about 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 be experienced in a woman's offline life. Women's experiences of violence whether it happens online or in person must be taken seriously.

The Digital Trail of Evidence

While experiencing technology-facilitated violence, some women have an idea of what technology is being misused by the perpetrator. 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, suspecting they may have access

to her device, accounts, or location via technology. Others may not even be able to identify the person who is harming them.

With technology-facilitated violence, 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 (i.e., devices, apps, and online accounts) a woman uses, and considering whether or how the perpetrator is using that technology to harm her, can be helpful in figuring out what technology is being misused.

Speaking with an anti-violence worker who understands technology-facilitated violence can help a woman determine what type of evidence she 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 Isn't the Problem

Technology-facilitated violence can be easier to document as it can provide a rich trail of evidence, and technology can be strategically used in safety planning. However, regardless of the methods, violence against women will always be the core issue of technology-facilitated violence. Technology misuse is one tactic among many that perpetrators use against women and this type of violence is usually not isolated. If technology was removed from the violent relationship, the abuse would likely continue in other forms of violence. BCSTH acknowledges that *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.

BC Society of Transition Houses

Technology Safety Project

This document is a part of a series that details how to preserve evidence related to the misuse of technology in experiences of domestic violence, sexual assault, and stalking. The series is part of the [Preserving Digital Evidence of Technology-Facilitated Violence Toolkit](). This document, or any portion thereof, may be reproduced or used in any manner whatsoever as long as acknowledgment to the BC Society of Transition Houses is included in the product.

This document was published March 2021.

Adapted with permission from the National Network to End Domestic Violence's Safety Net project, based on their [Legal Systems Toolkit]().

BC Society of Transition Houses

British Columbia

The Law Foundation of British Columbia