BC Society of Transition Houses

Preserving Digital Evidence:

Considerations for Anti-Violence Workers Supporting Women

Anti-violence workers are a valued source of support for women[1] experiencing technology-facilitated violence. They listen to and work with women to develop technology safety plans, including how to safely collect digital evidence, as part of their larger safety planning process. They play an integral role in supporting women responding to technology-facilitated violence.

Anti-violence workers center women's particular experiences in their support, as they know that women know their situation best and are often the most adept at creating a safety plan that makes sense for their situation.

As technology-facilitated violence is a relatively new phenomenon, anti-violence workers may be unaware of what is possible or necessary for preserving digital evidence, due to a lack of familiarity with the technology itself or the rules of the justice system. This unfamiliarity can have an effect on determining what is possible or necessary for preserving digital evidence, and which legal remedies are most relevant to a woman's case.

An anti-violence worker may follow the steps below to assist in strategizing a technology safety plan for a woman responding to technology-facilitated violence.

Step 1: Work with women 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, and particularly those used to communicate with the perpetrator;
- if and how perpetrators have access to technological device(s) or accounts (whether that be physical or digital access),
- whether there was any technology-related violence in their relationship and what the abusive behaviour was (threats, harassment, monitoring, posting negative comments),
- whether she suspects that the perpetrator may be accessing her devices, digital accounts or location secretly or without consent,

[1] In this toolkit we will be using the term "woman", "violence against women" and feminine 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 transgender, non-binary, male and female people. We hope that all people impacted by this violence will find these documents useful.

- 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 at risk of being lost or deleted, and
- the possible locations where the digital evidence of the technology-facilitated violence can be found.

For more information, see BCSTH's "Assessing for Technology- Facilitated Violence and Privacy Concerns for Anti-Violence Workers" information sheet.

Step 2: Protect the data

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

Next, it is important to determine where the digital evidence is currently stored (for example, in a text message on her phone; in an email on her personal email account, on a social media webpage, on her iCloud account) and to consider how to protect or freeze the data before actually preserving the digital evidence. This might include blocking the perpetrators access to accounts. It is important to be aware that, if an account becomes blocked, this can lead to the automatic deletion or access to the digital evidence. To block unwanted access to their personal accounts, women will want to change the passwords on all relevant platforms and devices.

A safety assessment should be done prior to 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 client and the strength of any future legal case she may choose to pursue.

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 (such as phones operating on the same system, tablets, laptops, desktop computers, fitness accessories, etc.) and will automatically sync information and backup 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 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 allows perpetrators to see what evidence is being preserved because they will have access to

texts, emails, videos and photos. Having remote access to cloud accounts also gives perpetrators access to destroy any evidence that is stored there.

Stalkerware is a type of malware which allows the perpetrator to monitor phone activity and track the location of the phone. If there are concerns that a device(s) is infected with stalkerware, it is important to create a plan on how to change passwords without alerting the perpetrator who may have access to the device's activities. For example, 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.

Digital evidence can also be lost through normal device and account functioning. In an effort 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 the digital evidence to remain stored on the device.

It is important to have a secondary backup of the 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 backup evidence.

Step 3: Explain limits to anti-violence worker's involvement in preserving evidence

Many anti-violence workers who are supporting women are asked to take photos and make recordings of technology-facilitated violence as a means to preserve evidence. They are also asked to store copies of digital evidence securely for their clients. Anti-violence organizations have records management policies that may address these types of issues. By personally assisting in digital evidence preservation, it may open up the risk that you or your client's file will be subpoenaed by the court. In some circumstances, this may be appropriate or necessary, however, clients should be encouraged to collect that evidence themselves or have a family or friend collect that data for them, whenever possible.

When a woman's digital evidence is preserved by an anti-violence worker, the organization may be required to testify in court as to the techniques used to preserve the evidence of the client, as well as the case notes in the client file. While photographic and digital evidence is very important for court matters, the authenticity of that evidence in court will be assessed based on steps taken by the person who preserved and stored that evidence. If an anti-violence worker collects digital evidence, they may be subpoenaed to explain how and why they collected the evidence. For example, an anti-violence

worker may be subpoenaed to testify in court that they were the one who documented and/or stored 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. If evidence is collected by the anti-violence worker, it is important that they discuss this risk with the client before collecting evidence.

Because of these risks, it is important to explain to women that preserving and storing digital evidence for them at the organization could have unintended consequences that might be detrimental for them in the long run. Many anti-violence programs have a records management policy of only recording the minimal amount of information necessary to provide the services needed for the time required. Check with the organization's policies, and if there is no policy, it should consider making one.

Anti-violence workers can work with women to discuss the possible consequence of having a third party, such as themselves, preserve evidence for them. 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.

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 out evidence. As part of the technology safety planning, anti-violence workers can provide women with resources which 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 which will be considered authentic and complete. Doing so will minimize opportunities which 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. Provide women with BCSTH's Technology-Facilitated Violence Log to help her keep a record of her 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 is useful for them to read the additional documents in our digital evidence toolkit to familiarize themselves with some of the technologies and techniques that will help their clients.

For more information about how to preserve and authenticate evidence, see the resources within this toolkit.

Step 5: Refer her to a legal advocate or lawyer

Women may need additional legal information or legal advice about ways to preserve digital evidence and relevant legal remedies. To find organizations in BC that provide legal information, legal aid, or legal assistance see:

- Rise Women's Legal Centre
- Legal Services Society
- PovNet

Step 6: Provide additional technology safety resources

BCSTH's Technology Safety Project has technology safety resources to assist your support of women experiencing technology-facilitated violence. See BCSTH's Technology Safety Project Resource page for information sheets on technology, legal remedies and safety planning.

Technology Safety Project

This document was published March 2021.

BC Society of Transition Houses

BRITISH COLUMBIA

THE LAW FOUNDATION OF BRITISH COLUMBIA