BC Society of Transition Houses

Safety Considerations for Women Preserving Digital Evidence

This first section of this handout focuses on safety considerations for women[1] **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 women should take into consideration when collecting this type of evidence. The first half of this handout discusses the importance of making a safety plan around evidence collection, which can help a woman avoid further abuse and can help save evidence from being lost. The second half of this handout provides tips on collecting digital evidence.

Women experiencing technology-facilitated violence often have access to large amounts of evidence of that violence. It is not uncommon for a perpetrator to send dozens, if not hundreds, of unwanted texts and emails. Many women will have received (and saved) abusive messages and other proof of violence from a perpetrator that can be useful to prove that she is experiencing violence. Sometimes she will automatically have a copy (for example, if her abuser sends an abusive email, she will automatically have a copy of that in her email folder). Other times, she will have to find a way to save it herself (for example, if her abuser posts a threat to her on his social media account she will need to screenshot it) or find it herself (for example, if her abuser has shared a nude image to a private messaging group she is not a member of she may need to try and get access to the image through someone else in the group). There may also be evidence on devices and online accounts that can help show what kind of violence she is facing and who is doing it to her, such as evidence that the perpetrator has had access to these things and it can be proven by showing which IP address or device accessed the account recently.

In experiences of technology-facilitated violence, sources of digital evidence include:

1. Evidence that women have direct access to, such as evidence on their devices and evidence that can be accessed through their online accounts. This can also include evidence provided through the accounts of people they follow or are “friends” with.
2. Evidence that other people have direct access to but the woman does not, such as information on the accounts of, or messaging apps of, friends of the perpetrator.
3. Evidence that perpetrators have access to, whether it is shared with the women, such as on a shared account, or the perpetrators have exclusive access.
4. Evidence that the woman may need technical support to gather, such as determining if stalkerware has been installed on her phone.
5. Evidence that needs to be obtained by court order or subpoena.

[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.

Consider Risks to Safety

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

If the perpetrator is alerted that evidence is being collected, there may be risk of violence escalating or critical evidence being deleted if the perpetrator is monitoring her behaviour on her devices or has access to her digital accounts or files. An example of this is when perpetrators have access to a woman's cloud storage account and is able to see that screenshots, photos, videos and conversations are being preserved and backed up to the cloud.

Connecting with a local anti-violence program[2] to assess the potential risks and develop a technology safety plan can help women safely strategize ways to preserve digital evidence. For example, anti-violence workers can help determine alternative ways to preserve evidence if a woman thinks that her abuser may become more violent if they can determine that steps have been taken to preserve the digital evidence of technology-facilitated violence. For example, they can help strategize how to collect evidence without alerting the abuser and ways to save (and backup) evidence effectively.

> *#TechSafetyTip* For more information about technology safety planning see BCSTH's technology safety planning guide and tip sheet.

Once a technology safety plan is developed, the following information provides guidance for evidence preservation.

Capture the Whole Conversation

Not all digital evidence will be admissible in court. However, capturing a full account of the available and relevant evidence is preferable, as complete records of the evidence is often required for it to be reviewed and considered credible in a court proceeding. Partial records, such as a single screenshot of a text conversation, can be subject to questioning and scrutiny as to why the entire piece of evidence (i.e., the whole conversation from that day) was not presented. For example, a lawyer for the other party

[2] For a list of anti-violence programs in British Columbia see https://bcsth.ca/directory/.

may ask you why you only showed this one text and ask you if you are hiding something by not showing the whole conversation. Showing the whole conversation allows the court to see the context of the text.

It is also important to capture the contact information of the person you are communicating with or is abusing you to show that it is them harming you. This can include showing a screenshot of their profile or contact information in your phone that shows their email or phone number. Having the phone number or email associated with the abusive messages can help prove it is actually them who was harming you.

A copy of all of the communication that identifies the perpetrator, their contact information, and their abusive behaviour can be helpful in experiences of harassment and stalking. This type of digital evidence can show a pattern and series of repeated events. Capturing the whole conversation can also give law enforcement a better understanding of what other evidence needs to be investigated.

> *#TechSafetyTip* Print out the conversation. Most courts prefer written (printed) copies. Some courts may not have the technology to play an audio or video recording on the day a person is in court, especially if they have not asked the court to have that technology available beforehand. You should check with the court beforehand if you are hoping to use audio or video evidence. If you are not able to print out the conversation (voice or video recording), you may need to have the digital evidence transcribed by a third party (i.e., have someone else type up exactly what was said so it can be printed for the court).
>
> *#TechSafetyTip* Make sure you collect information that ties the perpetrator to the technology-facilitated violence, such as their phone number, social media profile, or email. You will need to be able to identify who the person posting the content is in case the court or law enforcement wants to question them.
>
> *#TechSafetyTip* Avoid altering the document. There is no need to highlight, edit, crop, or reformat digital evidence. The courts often want to see the original document without any alterations. If there are alterations, it can cause problems with getting it admitted to court.
>
> *#TechSafetyTip* Consider creating a new email account that you only use for conversations with your perpetrator. This can help you keep track of all your conversations.
>
> *#TechSafetyTip* If communicating via email, start new email threads with new subject lines regularly. This can help streamline conversations and avoid irrelevant conversations from having to be submitted as evidence.

Time Is of the Essence

For some social media platforms, instant messaging services, voicemail messages and text message plans, digital evidence of harassment, threats and distribution of non-consensual intimate images are only available for a short period of time. For example, once the platform receives a complaint about the post, it might remove the comment or photo before you take a screenshot to show what was posted; or the account holder, where the information was posted, blocks you and you no longer have access to the messages or digital evidence; or the perpetrator realises they shouldn't have said what they did and they delete the post themselves before you make a copy of the post.

Though it may be difficult to do, it is important to capture digital evidence of violence before it is removed or deleted.

When considering safety, be aware that some apps like Snapchat notifies the account holder that a screenshot has been taken of that post or conversation. This may not be safe for some women to do, especially if they are concerned the perpetrator's violence will escalate if they think she is collecting digital evidence. You should look up the policies and practices of the social media company before taking screenshots to avoid this risk.[3] If the program does alert the other user to screenshots, consider taking a photo of the post with your phone or another recording device so the alert function is not triggered but you can still preserve the evidence.

> *#TechSafetyTip* Capture the entire post or message including the account owner/sender's name, available contact information, date, and time (if available).
>
> *#TechSafetyTip* Some text and instant message apps do not show the date and time stamp of a message sent and received on that current day. If this is the case, consider preserving the message again the following day so the date and time stamp is visible.
>
> *#TechSafetyTip* Use BCSTH's Technology-Facilitated Violence Log to document, record and keep track of experiences of technology-facilitated violence and digital evidence.

Records of Digital Evidence

Digital evidence, such as photographs of physical injuries or recordings of a harassing or threatening voicemail message, can be very important to proving a woman's case in court. It can be helpful to have a friend or other support person document and save evidence of the violence. Having others record,

[3] For example, the following social media platforms alert users when a screenshot is taken: (1) Snapchat; (2) Instagram notifies a user when their story is screenshotted; (3) Viber; (4) Telegram. In addition, keyloggers can be used to detect whether specific actions or a certain input were used.

preserve or transcribe digital evidence may not only be necessary to show what violence a woman is experiencing, but also as a strategic option to keep women safe. If the digital evidence has been taken, stored or transcribed by a third party, women should be advised that the third party, such as their friend or support worker, may need to testify in court as to their actions and the digital evidence they preserved and possibly submit an affidavit.[4] For example, they may need to tell the court that they were the one to take the photo of the woman's injuries.

Posting Digital Evidence Online

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

Preserving Digital Evidence

Once digital evidence has been preserved, it is important that it be saved somewhere safe. Women may want to save evidence on a phone, computer, or tablet that the perpetrator does not have access to. It may be helpful for women to change passwords on all their devices and accounts to prevent unauthorized access by a third party to the digital evidence.

For example, cloud-based accounts (such as iCloud or Google Drive) can be accessed by multiple devices, automatically save information in the cloud, sync information across several devices, and can back up data to multiple devices. Perpetrators may have access to a woman's cloud-based accounts by knowing passwords or having access to devices that have been set up with the joint account information on it. Women should identify if cloud-based accounts are linked to their device(s), and, where possible, which accounts perpetrators have access to. Access to cloud-based accounts allows perpetrators to view what evidence is being preserved and can provide them with the opportunity to remotely destroy any evidence that is being saved there.

Additionally, because there is always a risk to an account getting corrupted or a device getting lost or destroyed, women should back up their evidence on a second account or device and, if possible, keep a

[4] An affidavit is a document that contains facts that you swear under oath or affirm are true. For more information about how to write an affidavit see https://familylaw.lss.bc.ca/bc-legal-system/legal-forms-documents/affidavits/how-do-you-write-affidavit

printed hard copy of her evidence for her 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* Change passwords to all accounts and devices to make sure the perpetrator cannot access the digital evidence or other important information.
>
> *#TechSafetyTip* When preserving digital evidence, try to use a device that the perpetrators do not have access to.
>
> *#TechSafetyTip* Print digital evidence as soon as possible to prevent evidence from being destroyed remotely.
>
> *#TechSafetyTip* Digital evidence can also be compromised if a device is lost, stolen, or broken. Because accidents happen, make a plan for how to backup evidence.

Tell the Story

Women may need to show a combination of messages, posts, voicemail recordings and more to explain to law enforcement, judges and lawyers what is happening. As mentioned above, it is recommended to preserve all experiences of technology-facilitated violence. Women may want to keep a word document, spreadsheet, and/or binder that organizes the evidence in one place. Keeping the evidence stored and organized can provide a clear timeline and help explain, to the police and the legal system, what has happened to them.

Collecting and organizing digital evidence is helpful to:

- provide a record of what is happening, which is useful in pursuing legal remedies.
- alert women to any escalation or change in abusive behaviours such as an increase in monitoring, which may indicate that the situation is becoming more risky and the safety plan may need to be revised.
- assist women in seeing patterns in the technology-facilitated violence and determine, in detail, how perpetrators misuse technological devices and if there has been a breach of the woman's online security.

> *#TechSafetyTip* For more information on what to document in experiences of technology-facilitated violence, see BCSTH's Documentation Tips for Women experiencing Technology-Facilitated Violence handout

Working with a Legal Advocate or Lawyer

Technology misuse is a form of abusive behavior that regularly occurs in violence against women cases. Women often possess digital evidence of technology-facilitated violence before knowing how the evidence can be preserved and the possible legal remedies to hold perpetrators accountable. Part of a

woman's decision making in these matters may involve her preserving digital evidence to disclose to law enforcement. Doing so would be in support of an investigation of criminal charges in technology-facilitated crimes such as threats, criminal harassment, defamation, impersonation, coercion, extortion, the non-consensual distribution of intimate images, and voyeurism. Also, digital evidence may serve as support for legal proceedings such as obtaining a Peace Bond, protection orders in family court, conduct orders and even conditions of release in criminal matters. Digital evidence may act as compelling proof of technology-facilitated violence that is relevant to child protection matters or in court ordered mediation.

It can be complicated to know what evidence might be relevant for each of these legal matters. If possible, it can be useful to seek support from the legal community. Legal advocates, lawyers or law enforcement can help to identify and consider what digital evidence should be collected and what remedies might be available. Additionally, they can help identify what laws may apply that either:

- directly address the violence and abuse;
- explicitly or implicitly include the use of electronic communications; or
- relate to technology, communications, privacy and confidentiality, even if they are not necessarily focused on the underlying domestic violence or sexual assault.

By preserving evidence of technology-facilitated violence, a documented pattern of behaviour can be established which can be relevant to hold perpetrators legally accountable. This can directly increase the safety of women and their families. For more information, see the following BCSTH resources:

- Documentation Tips for Women Experiencing Technology-Facilitated Violence
- Sample Technology-Facilitated Violence Log

Working with Law Enforcement

When reporting a crime many women may not know what information to share, or may be concerned about giving the police access to private and potentially embarrassing information. Law enforcement departments have policies and protocols for collecting evidence. Women should have a conversation about this process with law enforcement before handing over evidence. For example, if a technological device, such as a smart phone, is provided to law enforcement for examination, a woman can ask what information they will be taking from the phone (i.e., downloading a copy of all information from the phone or only taking select photos and conversations),whether the device will be returned, and when.

If the device is considered a piece of evidence, the police may need to keep it for some time. Women may not have access to their devices or online accounts for a short or long period of time, which could have a direct impact on her safety and ability to communicate with her anti-violence worker, children, family and friends. This possibility should be discussed with the anti-violence worker and become part of the technology safety plan.

#TechSafetyTip Ask law enforcement what is most important for the investigation and for court. It is important to understand what is needed to move forward with a criminal investigation.

Once the digital evidence of technology-facilitated violence is preserved, it will be helpful to read the information sheets on authentication and relevance.

Meeting with law enforcement can be stressful, particularly if you are a member of a social group that may have had negative experiences with the police in the past. Black, Indigenous and people of colour have historically been disadvantaged in interactions with the police and may not see the police as a group that will help them, making reporting to the police an undesirable option.

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