BC Society of Transition Houses

Collecting Digital Evidence for Your Case

Fact Scenarios

These fact scenarios are meant to help people who are experiencing technology-facilitated violence and are thinking about seeking a legal solution to their problems. These scenarios will help you think about what digital evidence should be preserved and how to preserve digital evidence so that you can use it for your case.

It is important to note that the law is only one way that people try to resolve their problems involving technology-facilitated violence. We recommend that you use all of the resources available to you to find ways to end this abuse. You may want to get in contact with a victim services organization to help make a safety plan, especially if you are/were in a violent intimate partner relationship. Sometimes reporting to the police or beginning a civil case can result in escalated violence that you will want to safety plan around. If you are not aware of whom to talk to in your community, you can contact VictimLinkBC and their staff can connect you to a variety of services available to you including victim services, government services, transition houses, and access to justice resources.

Sometimes there may be technological solutions to preventing technology-facilitated violence. You can also read the Tech Safety Checklist to think of ways that can protect you from technology-facilitated violence. You may also find our Tech-Safety Resources sheet helpful. This resource lists organizations that are working in the area of technology-facilitated violence, many of which provide helpful guides on how to get help and increase your cyber security.

For those looking for a legal solution, the fact scenarios below will help you start thinking about how to plan your digital evidence collection and preservation.

You will want to consider what laws apply to your particular situation and what evidence may be needed to prove your case in court. It can be helpful to speak to a lawyer who can help you. If you are unable to afford a lawyer, a list of many of the laws related to technology-facilitated violence can be found [on our sheet on relevant laws].

It is important to keep more than one copy of your evidence stored somewhere. If it is only stored on your phone or computer and if the devices are lost or destroyed, or the files become corrupted, all of your evidence can be lost. See the Tech Safety tip sheet on Digital Evidence preservation for more information on how to preserve digital evidence.

Criminal Law

If you want to start a criminal case, you will need to report the perpetrator's criminal behavior to the police. You might also want to seek a peace bond against the perpetrator to protect you from future harms or to prohibit the perpetrator from sharing intimate images of you without consent. See the Tech Safety information sheet on Peace Bonds for more information on this procedure. It can be helpful to create a digital evidence log to keep track of the abuse over time and evidence related to that abuse. See the Tech Safety Digital Evidence Logbook as a sample.

When you go to the police to report the crime, you will want to bring evidence of that crime. It can be helpful to have the evidence printed out, but also to have copies of it digitally, such as on a USB stick to give to the police. Make sure you create a copy of this evidence for yourself to keep as well and write down a list of the evidence that you gave to the police. It can be helpful to talk to a victim service worker before going to the police so they can help explain what to expect when you report a crime to the police and what information to bring.

It can also be helpful if you know of laws you think the perpetrator broke so you can tell the police that you think the perpetrator may have broken these laws. However, this is not necessary, it is the responsibility of the police to know what the laws are and to know if they may have been broken. The police will ultimately decide which crimes to charge the perpetrator with if there is enough evidence to do so. They may even identify some laws that you did not consider.

In criminal court proceedings, as a victim you will not have an option to present the case in court yourself, so you will not need to present the evidence yourself to the court. Instead, the Crown counsel will be the lawyer who will present your evidence and you will provide evidence as a witness.

The Crown counsel is not your lawyer, but is the lawyer who represents the public interest. This means that solicitor-client privilege does not apply to your conversations with them, and instead, they have a duty to disclose information you share with them to the opposing side if it is relevant. You should ask them to explain their disclosure responsibilities before you provide them evidence.

You will need to give your evidence to the police, who will give it to the Crown counsel if a case is started or to the Crown counsel directly once they have been assigned to the case. Although the Crown counsel will be in charge of admitting evidence and asking you questions as a witness, it can be helpful to know what the rules of evidence are so you can understand why the Crown counsel is making certain decisions about evidence or asking you for different kinds of evidence. See the Tech Safety worksheet on Evidence and Objections for more information.

Civil Law

If you want to start a civil case (i.e., to sue someone for the harm they caused you), you will need to hire a lawyer to represent you or you can represent yourself. If you represent yourself in the case, you will need to file an application with the court to start a case. You will want to familiarize yourself with the rules of evidence. See our worksheet on Evidence and Objections for more information.

Family Law

If you and your ex-partner are involved in a family law case, you may need to prove that your ex-partner is engaging in family violence or other forms of technology-facilitated violence that make it difficult for you to feel safe or is impacting the well-being of you and your children. For family law cases, you can hire a lawyer or you can represent yourself. You may also be eligible for Legal Aid, and a free lawyer will be provided to you for a certain number of hours. If you are representing yourself, you will want to familiarize yourself with the rules around admitting evidence to court. See our worksheet on Evidence and Objections for more information.

Fact Scenario 1

My ex-partner has shared sexual images of me online.

Scenario

Imani and Jeff had been dating for two years. During their relationship, they enjoyed sexting and sharing sexual images with each other. Sometimes they made videos of the two of them having sex. They both promised not to share the images with anyone else and told each other this was something special, just for the two of them. This was really important to Imani because her parents were religious and would not approve of her having sex before marriage. Imani did not share her parent's beliefs about sex before marriage but she also did not want to rock the boat and does not want them to know she is sexually active. She knew if they found out it could really damage her relationship with her family who were very important to her. Jeff knew that she was always worried her parents would find out they were having sex.

Over the years, Jeff started being more and more controlling over Imani so she eventually tried to break up with him. He said that if she left him, he would send the pictures and videos to her parents. Imani did not want to stay in the relationship with him and didn't know what to do. Jeff said they had to have sex at least one more time or he would share the videos. Imani told him she did not want to but she would do it to stop him from sharing the videos. After they had sex for the last time, she told him their relationships was over. A few days later, she got a call from her friend Micha telling her that a video of

her and Jeff having sex was up on a pornography website with her name in the title of the video and that Jeff had sent the link to a group chat on Facebook that Micah, Jeff and several other friends were on, saying some really rude things about her. Imani is worried that he may post more of the images online and that her parents will find out about the video on the website.

Digital Evidence Collection

In this case Jeff could be accused of several crimes, including extortion, the non-consensual distribution of intimate images, and sexual assault. Imani may be able to sue Jeff for breaching her privacy and intentionally inflicting mental suffering on her.

Imani's first instinct may be to make a report to the pornography website where the video was posted non-consensually to get it taken down as soon as possible and to confront Jeff or delete him from social media. Before she does that she should collect as much evidence as possible that will help her in court. If she reports the video it can get taken down and the evidence will be gone, making it harder to prove that Jeff shared it in court. Once she has collected the evidence she needs, she should then report the video to try and get it taken down.

Evidence from her and Jeff's previous communications

- Imani should look back in all of her text, email and social media conversations with Jeff and take screenshots or make a screen recording of conversations where they had agreed to keep the images and videos they shared in their relationship private.
- She should take a screenshot of any conversation they had about the video, such as when it was made, who made it, if they shared it with each other and the conversations they had around the video, even if it might feel embarrassing to show the court because of its sexual nature.
- She should save a copy of the original video.
- She should take screenshots of any conversations they had where Jeff was upset about them breaking up and when Jeff told her they had to have sex again or he would share the photos or videos.
- She should take screenshots of any conversations they had where she told Jeff that it would be really upsetting for her if her parents found out that she was having sex before marriage.
- Imani should make sure that she collect not just screenshots of the conversations, but information that shows the dates and times of these conversations, as well as Jeff's profile information or contact information to show that the person who sent her those messages is actually associated with Jeff. For example, his contact information in your phone will list his

phone number that is associated with his cellphone account, which could prove it was actually him sending the messages.

- If she chooses to delete Jeff from social media or block his number, she should make sure she has downloaded all of their relevant communication beforehand. Some social media companies prevent you from accessing messages between you and a person once you are no longer following each other. See the Tech Safety tip sheet on collecting digital evidence for more information.

Evidence from her friend Micha

- She should ask her friend Micha to take a screenshot of the group chat message Jeff sent, including screenshots that show who all is in the group, the post with the link, and Jeff's profile or contact information related to his account. Imani will need to be able to prove not only that the link was posted to the group, but that it was Jeff who posted it. If Jeff uses a fake name or nickname on his profile, it will be important to collect other evidence that would show that Jeff uses that account, such as other posts on the account that have his photo or other information that could prove it is his account. It is important that this information get collected right away, as Jeff may delete it later.
- She should ask Micha for a copy of the link to the video that Jeff sent the group.

Evidence from the Pornography Website

- Imani should take a screenshot of the video on the website or make a recording of it with a camera or a program that would allow her to capture what is on her computer's screen. If there is information about the date, the user who posted the video, and how many times it has been viewed, she should screenshot that information, including whatever details she can get about the user's profile.
- She should take a screenshot of the name of the video and write it down.
- She should copy the URL of the video and save it in a separate document.
- She should take a screenshot of the length of the video.
- If there is any information that could link the posting back to Jeff, such as the username of the account that posted the video or the wording in the title of the video, she should document that. In many cases, images and videos are posted anonymously or under a fake name so it is more difficult to prove in court who posted it up. Imani should collect whatever information she can. In some cases, the police or the courts may be able to get a court order that will order the

website owner to provide more information about that particular account that can help identify who was associated with the user who posted the video.

Fact Scenario 2

My ex-partner is harassing me online

Scenario

Grace and Yael are in the middle of a heated custody battle over their son. Grace has been sending Yael texts and emails every single day, some of which she sends in the middle of the night. Some days it is more than 100 texts a day. Grace's messages are sometimes about their legal issues and arranging drop offs and pick-ups for their son, but a lot of them are Grace going on about the reasons she is upset that they broke up, and others are calling Yael names, saying she is a bad person, and that Grace is going to "get her" if she takes away their son. Some of the texts that Grace sends have information that Yael never gave to Grace and Yael is worried Grace might have hacked into her email. Yael has asked Grace to stop texting her so much and to only text her about their son.

Recently, Grace's behaviour has turned to the worse. Grace has been posting awful things about Yael on Facebook, saying that Yael is a terrible mother and is using the courts to turn their son against Grace. She has been following Yael and their son and filming them with her phone while they are at the park yelling at them that she is going to use this as evidence in their case to show that Yael is a bad mother. Grace has posted some of the videos on Facebook, and Yael is starting to feel afraid of Grace.

Digital Evidence Collection

In this case Grace could be accused of a crime, such as criminal harassment. Yael may be able to sue Grace for breaching her privacy and intentionally inflicting mental suffering on her. Because they are already involved in a family law dispute, Yael could seek a protection order that could limit Grace's contact with her. She may also decide to begin a criminal process by going to the police to try to get a Canadian criminal code peace bond.

Text Messages

- Yael will want to keep a copy of all the text messages Grace has sent her to show how excessive the texting has been. In a case like this it could be thousands of messages, which would be very tedious to screenshot each one. She can see if the messaging app has an option to export all of the texts at once. Otherwise, she can screen record or take a video of her slowly scrolling

through all the text messages, and then screenshot the texts that are relevant to her case in the future depending on the advice of the police, or her lawyer.

- She should make a note of and screenshot any date and time where Grace sent messages that were harassing, threatening, excessive, or made Yael uncomfortable. The court may or may not want to read every single message Grace ever sent so it is important to be able to have all of these messages saved somewhere. Once she or her lawyer have determined which are relevant to her case, she can then show the court those texts.
- She should make a note of and screenshot any date and time where she sent a message to Grace asking her to stop sending so many messages or that she was making Yael uncomfortable.

Email Messages

- Yael will want to keep a record of all of the emails that Grace has sent her.
- She should keep the original copy of all of the emails. These emails contain important meta data about when the email was sent and from whom. If the email is forwarded and then saved, it does not contain the metadata from the original message.
- She may want to create a special folder in her email account where she stores all of those emails. Because she is worried Grace has access to her email account she should make sure she also saves copies of these emails somewhere Grace doesn't have access to in case Grace does have access to her email and deletes the evidence.
- If she prints out the emails, she should print out all the messages that go back and forth on an email chain in one document. This will make it easier for the court to follow, compared to printing out each email and response individually.
- She should keep a second document, such as an excel spreadsheet or a word document, that makes notes of which emails contain what information and to make note of any emails that were harassing or threatening.
- She should also make note of any emails that she sent to Grace to tell her to stop sending so much communication or that it was making her uncomfortable.

Evidence of Unauthorized Access to Email

- Yael should go into her email account and look at the "Last Account Activity" or "Account Activity" to see if any unusual IP addresses are accessing the account. Yael will need to know her own IP address and will need to remember if she has used other internet connections, such as her work place or a coffeeshop, in order to cross reference the IP addresses listed on the account.

- If there are unidentifiable IP addresses, Yael should take a screen shot of this, as it might help show that Grace has been accessing her email if one of the IP addresses that accessed her account is Grace's. However, if Yael doesn't know what Grace's IP address is, it may be difficult to find out Grace's IP address is. Yael may need to get assistance from the police or the court to do this. This information can be very difficult to get. Yael will need to bring evidence of why she thinks Grace is accessing her emails, such as any of the texts or emails that mentioned things that Grace could only know if she had access to Yael's email.

Evidence of Facebook Messages

- If Yael is friends with Grace on Facebook and can see the posts herself, she should take screenshots of the posts that Grace makes about Yael, including the posts of the videos Grace has filmed of Yael and their son.
- She should make sure the screenshot includes the date and time of the post and information that can prove the account belongs to Grace. The evidence will need to show a connection between Grace and the posts.
- She should take a screenshot of the profile information associated with the account. If Grace uses a fake name on her profile, it will be important to collect other evidence that would show that Grace uses that account, such as other posts on the account that have her photo or other information that could prove it is her account.
- If Yael is not friends with Grace on Facebook, she may need to ask a friend or a family member to collect this evidence on her behalf. She may need to ask that friend to act as a witness if the case goes to court.

Evidence of Unwanted Filming

- Yael should keep a record of the times and dates when Grace is filming her.
- She may want to take a photo or video of Grace filming her. However, Yael will want to consider whether this will escalate the situation or not. There is a risk that the court may think that she is part of the problem if she is also filming Grace. It might be more useful to have a friend come with her to the park so that both she and her friend can make a statement to the court about Grace's filming.

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.

We gratefully acknowledge Suzie Dunn, PhD Candidate at the University of Ottawa for the creation of this information sheet.

BC Society of Transition Houses

THE LAW FOUNDATION OF BRITISH COLUMBIA