



LEAF
FAEJ

**WOMEN'S LEGAL
EDUCATION & ACTION FUND**
**FONDS D'ACTION ET D'ÉDUCATION
JURIDIQUE POUR LES FEMMES**

Unacceptable: Responding to Technology-Facilitated Gender-Based Violence

This guide contains information on the growing phenomenon of technology-facilitated gender-based violence, including steps to address it, and links to resources for more information and support.

This publication is supported by the Department of Justice Canada, and was created as part of the Victims and Survivors of Crime Week 2021.

1. About this Guide

This guide contains general legal information for people living in Canada. The information contained in this publication is current as of October 2021 and does not constitute legal advice for a specific legal problem.

Copyright © 2021 Women's Legal Education and Action Fund (LEAF)

Published by:

Women's Legal Education and Action Fund (LEAF)

180 Dundas Street West, Suite 1420

Toronto, Ontario, Canada M5G 1C7

www.leaf.ca

This guide was prepared by Rosel Kim, Staff Lawyer and Lead, LEAF's Technology-Facilitated Violence Project. Thank you to Moira Aikenhead, Suzie Dunn, Raine Liliefeldt, and Nasreen Rajani, who provided helpful suggestions.

2. About LEAF

LEAF is a national, charitable, non-profit organization that advances substantive gender equality through litigation, law reform, and public education. Since 1985, LEAF has intervened in over 100 cases – many of them before the Supreme Court of Canada – that have advanced gender equality.

3. Learn more about technology-facilitated gender-based violence (TFGBV)

Technology-facilitated gender-based violence (TFGBV) refers to a wide range of unacceptable, violent, and abusive behaviours, where technology (such as a phone, computer, Smartwatch or a Smart home device) is used as a central tool to carry out these behaviours. This section will discuss different types of acts that qualify as TFGBV, which may be difficult and triggering for some to read.

TFGBV is unacceptable because it violates your dignity, your equality rights, your privacy, your security, and your freedom of expression. This is why it is important to recognize the serious harms caused by it, name the behaviour accordingly, and speak out against it.

Much of TFGBV happens on digital platforms. **Digital platforms** (or online platforms) refer to websites or apps, which include: social media platforms (Facebook, Twitter, Instagram, TikTok, Reddit, OnlyFans); blog sites (Wordpress, Blogger); video-sharing or streaming sites (YouTube, TikTok, Twitch, OnlyFans); dating apps (Tinder, Grindr, Hinge); pornography or sexual service platforms (PornHub, XVideos); payment processors and crowdfunding platforms (Patreon, PayPal, GoFundMe).

If you are experiencing any of the behaviours described below, you are experiencing TFGBV:

- **Coordinated flagging:** deliberately misusing a digital platform’s mechanisms for reporting abuse in order to disrupt or silence your online presence or content. This can include a group of individuals organizing to ‘flag’ or report your posts for removal or reporting your account to be suspended, claiming you or the content you posted violated the platform’s community standards or terms of use.
- **Deepfakes:** creating realistic video or audio using artificial intelligence (AI), where you are seen or heard saying or doing something that you did not actually say or do in real life. Most deepfakes online are manipulated pornographic images where the face of the person in the video has been swapped out with someone else’s face.
 - “**Cheapfakes**” or “**shallow fakes**” refer to video or audio that has been manipulated without the use of AI, such as having the timing slowed or the background changed to alter how the video is perceived.
- **Defamation:** when someone posts something untrue about you online that would negatively impact your reputation.
- **Doxing, or doxxing:** when your personal information (such as your full name, home address, social insurance number, bank account information) is disclosed online without your consent.
- **Hate speech:** in Canada, hate speech has specific legal requirements. In order to qualify as criminal hate speech, the person making the speech must have “willfully promoted” hatred against a group.

- **Impersonation:** when someone pretends to be you.
- **Non-consensual distribution of intimate images (NCDII):** when someone shares a nude or sexual image of you without your consent. The sharing can take place online, and/or in private messages sent to other people. This is also referred to as image-based sexual exploitation or image-based sexual abuse.
- **Online harassment:** when someone engages persistently with you online in a way that is unwanted.
- **Online mobbing or swarming:** when many people simultaneously coordinate online harassment or online abuse against you.
- **Online sexual harassment:** a type of online harassment that focuses on, or references, your sexual activity, sexual history, and/or sexuality. One common type of online sexual harassment is slut-shaming, where the harassment concentrates on your sexual history and/or activity.
- **Sextortion:** when someone attempts to sexually extort you by capturing sexual or intimate images or recordings of you, and threatens to distribute them without your consent unless you follow their orders (such as orders to pay them or perform sexual acts).
- **Spyware/stalkerware:** when someone uses apps or devices that can spy on, and/or monitor you through mobile phones and/or computers. The spyware/stalkerware gains access to your device's camera, or the location information on your phone and/or computer and transmits that data to your abuser.
- **Swatting:** named after police Special Weapons and Tactics (SWAT) teams, swatting involves someone calling 911 or law enforcement to make a false report about you doing something dangerous or harmful (like holding a hostage or owning a weapon), in order to send police officers (or a SWAT team) to your location.
- **Technology-aggravated sexual assault:** sexual assault with an online component – i.e., a group of people filming themselves sexually assaulting someone and posting the video on social media.
- **Threats to you or to people close to you (including family and friends):** this can include rape threats and/or death threats.
- **Trolling:** when users post messages, images, videos, or otherwise online content, or create online campaigns (such as hashtags on Twitter) to annoy you, cause disruption in your life, and/or incite violence against you.

Many trolls are anonymous and use fake accounts on digital platforms, meaning these accounts are not associated with their real names or identities.

- **Voyeurism:** when someone secretly observes you or records you (by accessing your webcam or phone camera without your consent or knowledge, or through a hidden recording device) while you are in a situation that you expect to be private– i.e., when you’re engaged in sexual activity or are at home.

Why TFGBV?

In our work, we use “technology-facilitated gender-based violence” or TFGBV in order to explicitly name the violence, and to note the central role of technology in perpetuating the harm.

We avoid attaching the prefix “cyber- ” to existing terms (such as “cybermisogyny” or “cyberviolence”), because it can indicate that what happens online is separate from, or less serious than, our “offline” lives, which is a false distinction. Our online lives are integral to, and cannot be separated from, our offline lives. Technology is also a more encompassing term that includes technologies that are not connected to the internet, such as a recording device.

Additionally, we avoid using the term “revenge porn” because it focuses on the motivation of the aggressor (i.e., to seek revenge on the victim/survivor) as opposed “non-consensual distribution of intimate images”, which names the harmful behaviour.

For more in-depth discussion of TFGBV, read LEAF’s research report “[Deplatforming Misogyny](#)” by Cynthia Khoo.

4. What can you do if you’re experiencing TFGBV?

If you are experiencing TFGBV, remember that what you’re experiencing is not okay, and that what happened is not your fault. You can choose a path forward to addressing the violence and healing in a way that works for you; the law may be one tool that you can use to stop the TFGBV and/or potentially hold the person doing these acts accountable.

- a. Seek and form a support network
 - Regardless of your choice of action, you can connect with other survivors to build networks of support by reaching out to other people you trust, reaching out to crisis support centres, and consulting other available resources. See Section 6 for a list of resources that can be helpful for gathering more information and support.
- b. Keep a record of the TFGBV incident(s) and the report(s) you make
 - Keep a record of the TFGBV and the reports you’ve made about it. You may need to use the record for further legal action if the platform does not respond and/or remove the TFGBV-related content.

- If record-keeping is too triggering and laborious, ask someone you trust for help.
 - Make sure you collect this evidence before you report the content to the social media platform. If you report it before capturing the evidence, it may get deleted by the social media company before you have time to document it.
 - If possible, take screenshots of the TFGBV with your phone and/or laptop, and document as much detail about what happened.
 - In your record-keeping, ensure that your records are kept securely and privately, especially if you suspect someone is monitoring your technology devices and/or email/social media accounts.
 - See this [Sample Technology-Facilitated Violence Log](#) prepared by the [BC Society of Transition Houses](#) for a suggested format.
- c. Use the platform's internal reporting tool to report TFGBV-related content and request for its removal
- Many platforms have codes of conduct and/or terms of service that apply to their users. This can include internal reporting mechanisms where users can report content that violates the code of conduct or the terms of service. You can report many forms of TFGBV-related content to the platform for violating the codes of conduct in order to get it removed.
 - If possible, ask people in your network to report the content as well, because multiple reports can lead to faster review of the flagged content/action from the platform.
- d. Consider legal action
- Depending on the type of expression and content that was posted, the perpetrator of TFGBV may be subject to criminal or civil sanctions. This section discusses factors to consider for both criminal and civil proceedings.
 - If you are considering legal action, know that legal proceedings can be a slow and lengthy process. In addition, because the law changes slowly, it has not caught up with all the ways in which TFGBV has resulted in serious harm to women and gender diverse people.
 - If you are thinking of pursuing legal action, ask the following question first:
 - *What kind of outcome are you looking for?*
 - A criminal conviction can lead to punishment for the perpetrator, including imprisonment (though not all criminal convictions will lead to imprisonment).
 - A civil claim can lead to compensation for you as a survivor if you are successful. In a civil suit, you can also ask for an injunction, where the court can order someone to do something (such as stop distributing intimate images, or remove their content).
 - If you're thinking of pursuing a criminal proceeding:

Reporting TFGBV to the police may be a time-consuming and resource-intensive experience. However, you are entitled to have your case be taken seriously by the police and the police should gather evidence for your case. The following questions may assist you in deciding if a criminal proceeding is right for you:

- *Does your experience fit with an existing criminal offence?* To start the proceeding, you will need to report the incident to the police, who will determine if the TFGBV you are experiencing meets the definition of a criminal offence in the *Criminal Code*. Some clearly harmful behaviour may not qualify as a criminal act. See Section 5 for more details on criminal offences that may correspond with the TFGBV you are experiencing.
- *Are you comfortable with sharing details about yourself and the TFGBV you experienced with the police?*
 - In some cases, a police officer may not be familiar with some of the new laws that do apply to TFGBV.
 - Black, Indigenous, and racialized communities are criminalized at a disproportionate rate. If you identify as Black, Indigenous, or racialized, you may not trust the justice system and/or have much desire to engage with the justice system as a tool to resolve TFGBV.
 - When you go to the police to report the incident, they will likely ask you to provide detailed information about you and what happened, including:
 - Your personal information (name, date of birth, address, contact information, social media usernames if relevant)
 - Copies of the content you would like to report (i.e., screenshots of the text messages or content and/or images that have been shared). You will need to be able to show when they were sent and to whom. They might require you to take screenshots of the timestamps of the messages and the actual contact information of the person who shared them, such as the phone number associated with the name in your phone contact list.
 - Timeline of events, including details about how the content was shared.
- *Are you okay with law enforcement and the Crown lawyers making decisions about your case?*
 - Once you contact law enforcement about your case, decisions about your case will be made by the police and the Crown lawyers

(lawyers representing the government) who will decide to prosecute the case or not; you may have minimal involvement other than providing evidence about your case. The Crown lawyer does not represent survivors directly (i.e., the Crown lawyer is not the survivor's lawyer).

- Once the police lay a charge against the perpetrator, the Crown lawyers will decide whether the charge should lead to a criminal trial.
 - Survivors of sexual and gender-based violence have faced barriers in reporting sexual assaults to law enforcement and engaging in the criminal justice system. [Statistics Canada's review of court outcomes of police-reported sexual assaults](#) found that only 21% of sexual assaults reported by police led to a completed court case. Many forms of TFBGV are sexual in nature, and may face similar barriers when reporting.
- *Are you okay with the possibility of facing invasive questions from the defence, if your case goes to trial?*
 - If your case goes to trial, you could face very detailed and potentially invasive questions from the defence lawyer representing the accused, which could lead to re-traumatization.
- If you are thinking of pursuing a civil proceeding:

Unlike a criminal proceeding, you will be a direct party in a civil claim (i.e., the lawyer will represent you and your interests), which allows you to have more control over the process. If you're considering a civil suit, ask yourself the following question:

- *Are you willing to spend some time and money?* Litigation, especially civil litigation, can take a long time to schedule and conclude. In addition, paying for a lawyer to represent you can be expensive. If your claim is not successful in court, you may be ordered by the court to pay for the costs related to the claim for the other party (including the other party's legal fees).
- How can you find a lawyer who could assist and/or represent you?
 - If you are looking for a lawyer, you can use a referral service offered by the law society of the province or territory you live in. Law societies are professional associations regulating legal professionals. Law societies maintain a public database of licensed legal professionals that you can search. Some law societies also provide a referral service (either by phone and/or online) that could match you with a lawyer with relevant subject-matter expertise.

- Depending on the TFGBV you're experiencing and the remedies you are seeking, you may wish to look for a lawyer specializing in privacy law, criminal law, and/or civil litigation.

5. What are potential legal remedies for victims/survivors experiencing TFGBV in Canada?

Because TFGBV encompasses a broad range of behaviours, there are different legal options for survivors. If you decide that legal action is the right option for you, see some of the laws that might apply to your situation below.

This section provides a brief and general overview of potential legal options for informational purposes only, and does not constitute legal advice. Specific legal questions and issues should be discussed with lawyers.

Criminal law

If a crime has been committed against you, you are entitled to fair treatment by the police and the criminal justice system. As mentioned above, you may be required to provide evidence of the crime and testify at a criminal trial. A criminal conviction can lead to punishment for the perpetrator, including imprisonment. However, not all criminal convictions lead to jail time.

Many acts of TFGBV could meet the definition of the following criminal offences in the *Criminal Code*:

- Criminal harassment (section 264(1))
- Defamatory libel (section 298(1))
- Extortion (section 346)
- Hate speech (section 319(2))
- Harassing communications (section 372(3))
- Identity fraud (section 403)
- Intimidation (section 423(1))
- Mischief in relation to computer data (section 430 (1.1))
- Non-consensual distribution of intimate images (section 162.1)
- Uttering threats (section 264.1(1))
- Voyeurism (section 162(1))

Civil litigation

You also have the option of bringing a civil lawsuit against the person who carried out the act of TFGBV. In order to bring a civil suit, you should connect with a lawyer who can represent you.

Filing a complaint with the privacy commissioner

Depending on where you live in Canada, you may be able to file a complaint with the Office of the Privacy Commissioner of Canada (OPC), which enforces Canada's federal privacy laws. In provinces where the *Personal Information Protection and Electronic Documents Act* (PIPEDA)** applies, you

could file a complaint with the Office of the Privacy Commissioner of Canada (OPC), stating that a company (such as a company running a pornographic website or a digital platform) violated its privacy obligations under *PIPEDA*. If the company is not Canadian, you would need to prove that the company has a “real and substantial” connection to Canada.

If the OPC agrees that the company has violated its privacy obligations disclosing your personal information without your consent, the OPC can make a recommendation that the company remove the personal information and change their practices.

For many years, the OPC (and other privacy experts) has been calling for a substantial reform of the *PIPEDA*, so Canada’s privacy laws may change significantly in the near future.

****The *Personal Information Protection and Electronic Documents Act (PIPEDA)* regulates the use of personal information by private sector organizations (such as companies) during the course of commercial activities. *PIPEDA* applies to private sector organizations in all provinces and territories except for Alberta, British Columbia, and Quebec. In Ontario, *PIPEDA* applies to all use of personal information except health information.**

6. Resources

If you are experiencing TFGBV, the following resources may be able to provide more information and support:

LEAF Resources:

- Visit [LEAF's Technology-Facilitated Violence Project's](#) webpage to learn more about LEAF's advocacy in this area, including case law and law reform submissions.
- Read the [Deplatforming Misogyny](#) report to learn more about the role of digital platforms in perpetuating TFGBV, and what should be done to hold platforms accountable.

National Resources:

- **BC Society of Transition Houses' (BCSTH) Tech Safety Program**
 - BCSTH's Technology Safety Project develops resources and information on the use of technology for Canadian anti-violence organizations and women experiencing technology-facilitated violence: <https://bcsth.ca/technology-safety-project-resources/>
- **Cybertip.ca (for people aged 18 or younger)**
 - This is Canada's national tipline for reporting the online sexual exploitation of children. In Canada, companies providing internet services are required to report online child pornography to the Cybertips.ca program and to law enforcement.
 - If you are under 18 years old and would like to report someone sharing an intimate image of you that was shared without your consent, you can report the incident or get more information about available legal options at: https://www.cybertip.ca/app/en/report-sharing_sexual_pictures

- **The eQuality Project**
 - The eQuality Project is dedicated to the creation of new knowledge about young people's use of networked spaces, with special emphasis on privacy and equality issues. Visit their criminal case law database to learn how the criminal law can respond to TFGBV: <http://www.equalityproject.ca/resources/tfv-criminal-case-law/>

Nova Scotia:

- **CyberScan**
 - CyberScan staff, who are members of the Public Safety Division of the Nova Scotia Department of Justice, help victims find a solution. They can contact the person responsible for the sharing of intimate images without consent or cyberbullying to informally resolve the issue. They can also help individuals navigate the justice system, explain legal options and offer support: <https://novascotia.ca/cyberscan/>

For more information or questions about this publication, contact:

Rosel Kim

Staff Lawyer and Lead, Technology-Facilitated Violence Project

r.kim@leaf.ca