# What is Technology-Facilitated Gender-Based Violence?

### A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

Technology-facilitated gender-based violence (TFGBV) is when technology is misused by perpetrators to commit violent abusive acts such as domestic violence, harassment (stalking), sexual assault, impersonation, extortion, and the non-consensual filming and sharing of intimate images. It can include things like receiving threats or harassment over text message or social media, location tracking or surveillance using technology, restricting access to technology, or online sexual exploitation and harassment.

Abusers are increasingly misusing a variety of phone, surveillance, computer technologies, apps, and social media platforms to harass, threaten, coerce, defame, intimidate, and monitor women and girls.

It is common for a perpetrator to misuse multiple technologies at once while also using more traditional power and control tactics such as withholding access to children and/or finances.

## What Does Technology-Facilitated Gender-Based Violence Look Like?

The following is a list of the most common forms of technology-facilitated gender-based violence. This is not meant to be an exhaustive list. For more details on different forms of TFGBV, check out the specific tip sheets and guides in the Technology Safety and Privacy Toolkit.

**Harassment:** the misuse of technology by a perpetrator to repeatedly contact, threaten or intimidate another person when they do not want them to and it makes them feel afraid.

This may be happening to you if you're:

- Being sent abusive, threatening, or insistent text messages and/or emails.
- Receiving persistent Facebook, WhatsApp, Snapchat, or other online platform messages.
- Continually being tagged on social media such as Instagram or Facebook.
- Receiving posts of abusive and/or continuous comments and replies to social media posts.

**Stalking/Criminal Harassment:** misusing technology to knowingly and/or recklessly harass someone that causes that person to reasonably fear for their safety or the safety of someone they know.

In Canada, this includes:

- Repeatedly following a person from place to place or following anyone known to the survivor;
- Repeatedly communicating, either directly or indirectly, with the survivor and/or anyone known to them.
- Harassing, disturbing, or watching the survivor's house or place where they, or anyone known to them, resides, works, carries out business, or happens to be; or engaging in threatening conduct directed at the survivor or anyone they know.

This may be happening to you if the perpetrator is:

- Using apps, location trackers, or stalkerware to learn your whereabouts and/or follow you from place to place.
- Using technology (e.g. apps, social media, texts, instant messaging) to repeatedly communicate with you directly or indirectly.
- Using webcams, hidden cameras, or apps to watch you at your home, work, or as you carry out your daily business.

**Impersonation:** hiding behind technology to pretend to be someone else as a tactic of further violence and control, for example, to damage a woman's reputation or relationships.

This may be happening to you if:

- You receive replies from strangers regarding an unknown advertisement that links them to you as the person who posted the ad.
- You receive angry responses from friends and family regarding messages, emails, or communications that you did not write.
- Your employer receives an unauthorized resignation email seemingly from you.
- You receive communication from a perpetrator impersonating a new partner or friend to "catfish"/ get close to you and connect with you.
- You receive notifications that your accounts are closed or you've changed passwords or cancelled your utility accounts when you have not made any changes to your accounts.

**Monitoring/Surveillance:** the misuse of technology to learn, know about, or follow another person's communications or activities. This can be possible if a perpetrator has physical or remote access to a device.

This may be happening to you if the perpetrator is:

- Logging onto your smartphone, email, or social media accounts to monitor your activities.
- Using apps, spyware, or key-stroke loggers to learn your location.
- Inserting a GPS tracker into your car or GPS-enabled watches and other accessories.
- Using hidden cameras that have been installed or strategically placed.

**Location Tracking:** using apps or tools to track a person's location, such as stalkerware. It may seem like the perpetrator knows where the person is at all times.

This may be happening to you if the perpetrator:

- Is using apps, location trackers, or stalkerware to learn your whereabouts and follow you from place to place.
- Has access to your cloud accounts and your smartphone has location services turned on.
- Has apps on your phone such as "find my friends" turned on and is a member.
- Gives location tracking technology to your children through a smartwatch, AirTag or Tile, or phone apps.
- Has access to GPS systems in your car.
- Is misusing family and friend location capabilities found on technology-enabled devices.

**Threats:** the use of language threatening to harm, extort, or humiliate someone through the use of technology.

This may be happening to you if you're:

- Receiving threats that the perpetrator will post personal information, photos, videos, or other material unless you comply with their demands.
- Being locked out of social media, email, or other online accounts including banking.
- Receiving threats through text, email, and social media.

**Non-Consensual Distribution of Images:** distributing, sharing, and posting private/intimate photos and videos of a person without their consent.

This may have happened to you if:

- Intimate and private images or videos of you have been posted online without your consent to embarrass, humiliate, harass, degrade, and/or harm.
- Private/intimate photos or videos of you have been sent to your friends, family members, employers/coworkers, and/or strangers without your consent.

**Consent** means an ongoing process of **giving and receiving permission.**

**Doxing:** the publication of private or identifying information of a particular individual on the Internet without the individual's consent.

This may have happened to you if:

- Your personally identifying information (e.g. name, address, phone number, email address, passport/SIN numbers) was posted on social media or websites without your consent.

*Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.*

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada
Femmes et Égalité des genres Canada
Canada