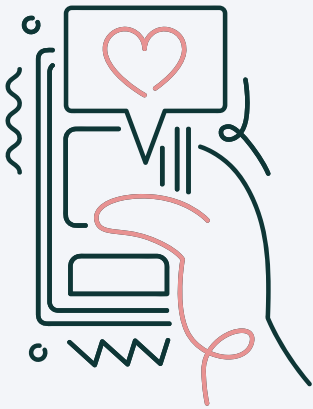


Technology-Facilitated Violence

against women & gender diverse candidates & politicians during the 2023 PEI provincial election



Technology-Facilitated Gender Based Violence (TF GBV) Defined:



Any act that is committed, assisted, aggravated or amplified by the use of information communications technologies or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms against a person on the basis of their gender.

TF GBV Trends

PEI candidates

- frequently did not report incidents of TF GBV to their party out of concern the party was ill-equipped to handle the incident
- expressed relief that their experiences of TF GBV did not escalate beyond the virtual
- learned there was often little the RCMP were able to do when they reported an incident of TF GBV

What We Heard

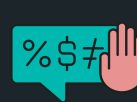
Anonymous quotes from candidates who agreed to a campaign de-brief with us

“A fellow candidate encouraged me to report the threat I had received to the local authorities, so I provided them with screenshots. I don’t know if anything came of it.”

“I did get threatened. A guy must have found my personal email, I don’t know how. There were thinly veiled physical violence threats, with a lot of cursing. I determined which district he was from so we avoided his house and the area. I was told to maybe call the RCMP, but nothing further.”

“Someone either hired a bunch of Twitter bots to spam me with insulting replies and or an anti-mask/anti-LGBT+ group found me and decided to target me. Some of the Twitter accounts were from PEI but most were not local as far as I could tell. I didn't report it to the party, mostly because this incident happened on election day and I just ended up blocking or muting the accounts.”

FORMS OF TFV



Online harassment: The use of technology to repeatedly contact, annoy, threaten or scare someone. This can be perpetrated by a single individual or mobs of people.

Cyberstalking, tracking or pursuit and surveillance: The use of technology to stalk and monitor someone's activities and behaviours in real-time or historically.

Image based abuse (IBA): Using images to coerce, threaten, harass, objectify or abuse. This involves taking, sharing, or threatening to share intimate and or sexual images without consent.

Doxxing: Non-consensual public release of personal information. It can include an individual's private, personal, sensitive information, such as home address, phone numbers, employer and family member's contact information.

Hacking: The use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the person targeted.

Impersonation: The process of stealing someone's identity so as to threaten or intimidate, as well as to discredit or damage a user's reputation. This does not include clearly described parody accounts.

Cross platform harassment: Coordinated and deliberately deployed harassment against a target, by a single harasser or a group of harassers, across multiple online communication platforms, taking advantage of the fact that most platforms only moderate content on their own sites.

Information communications technologies: Computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (e.g. fixed or mobile, satellite and visio/video-conferencing).

IRL-attacks: Incidents where online abuse either moves into the 'real' world or is already part of an ongoing stalking or intimate partner violence interaction.

Deep fakes: Digital images, videos and audios that are artificially altered or manipulated by AI and or deep learning to make someone appear to do or say something they did not actually do or say.

Summary of Policy Recommendations

Education: teach all candidates, campaign teams and volunteers the definition of technology facilitated violence to ensure they know how to identify it. Provide social media training and how to use platforms. Training should emphasize when to block, delete, mute or reply to comments and messages, explaining the benefits and repercussions of these decisions.

Standardized codes of conduct for online interactions: publicly list the guiding principles set by the party or individual to identify and manage interactions. Should a candidate face pushback from a citizen for blocking or deleting, refer them to the rule they violated.

Document and report: designate a person responsible within the party to receive reports of technology-facilitated violence, and establish a mechanism where candidates can submit screenshots and other evidence of the incident. Track the type and frequency of the technology facilitated violence.

Penalties: outline the consequences for individuals within the party who engage in technology-facilitated violence, such as fines, legal action, or expulsion from the party. Those on the receiving end should be allowed to pursue legal action if it is deemed necessary.

Support for victims: provide support and resources for victims of technology-facilitated violence, including access to counselling, legal assistance, and other support services.

We thank the Interministerial Women's Secretariat for supporting this project through their fall 2022 Violence Against Women Prevention Grant.