

TECHNOLOGY AND GENDER-BASED VIOLENCE

In a survey of victim services providers, 97% indicated that victims who seek their services were being harassed, monitored, or threatened by perpetrators misusing technology.ⁱ More recently, a 2022 survey by the National Domestic Violence Hotline found that 100% of respondents experienced at least one type of online abuse and/or harassment.ⁱⁱ Understanding the impact of abusers' misuse of technology, the types of technology misused, and the ways in which technology can be used to assist survivors is therefore crucial to providing survivor support.

While harassment, threats, and intimidation are not new tactics in the world of stalking, domestic violence, and non-partner sexual violence, abusers are increasingly using technology to monitor, harass, threaten, intimidate, impersonate, and stalk their victims, making it difficult for victims and survivorsⁱⁱⁱ to find physical safety and eroding their sense of safety. It is not uncommon for abusers to misuse multiple technologies at once, while also using non-technological abusive tactics.

YWCA recognizes that not all types of violence and abuse are recognized or responded to equally. Survivors of some types of abuse, particularly newer forms of abuse using ever-changing technology, face difficulties in gaining access to justice where legal systems have not yet caught up to technological shifts. As the largest network of domestic and sexual violence service providers in the country, YWCA is dedicated to promoting women's health and safety through direct services, advocacy, and issue education.

FACTS

- Technology-facilitated gender-based violence (TF GBV)^{iv} is violence that is facilitated by the use of information and communication technologies, or digital media, and includes, but is not limited to:
 - Online violence – violence that occurs in online spaces, such as non-consensual sharing of intimate images, private communications, or personal data; image-based sexual abuse; tech-facilitated sexual abuse; online harassment and abuse; and targeted hacking; and
 - Offline violence – violence perpetrated through technological means, but which is not typically thought of as “online violence,” such as using technology for surveillance, monitoring, control, and stalking.^v
- Most TF GBV is perpetrated by someone known to the victim, either as an intimate partner or as someone belonging to the survivor's immediate social circle.^{vi}

TF GBV is prevalent, and highly gendered.

- Young women, women who regularly engage in online spaces, and LGBTQ+ individuals are disproportionately targeted by TF GBV.^{vii}
- Globally, online violence against women is prevalent, with 38% of women reporting personal experiences with online violence, 65% reporting they know other women who had been targeted online, and 85% reporting witnessing online violence against other women. Younger women (Gen Z and Millennials) are more likely to personally experience this violence compared to Gen X and Baby Boomer women (45% versus 31%).^{viii}
- Online: Globally, survivors of online violence most often report experiencing misinformation and defamation (67%), cyber harassment (66%), hate speech (65%), impersonation (63%), astroturfing (58%), video and image-based abuse (57%), doxing (55%), and violent threats (52%), and the receipt of nonconsensual sexually explicit images and content (43%).^{ix}
- Offline: More than 80% of stalking survivors report that some form of technology^x was used to stalk them; electronic monitoring of some kind is used to stalk 1 out of every 2 stalking survivors.^{xi}

Harms of TF GBV

- While survivors of both non-technological abuse tactics and technology-related violence engage in many of the same protective behaviors, survivors who experience technology-based stalking are more likely to take time off from work; change or quit their job or school; avoid relatives, friends, or holiday celebrations; or change their email address when compared to other survivors. They also experience greater fear over time.^{xii}
- TF GBV also harms survivors' mental health, including through depression, general anxiety disorder, the doubting of one's sanity, and suicidal ideation. Of all forms of TF GBV, non-consensual image sharing is believed to have the most traumatic and long-lasting mental health impacts, which are often coupled with social and economic consequences.^{xiii}
- The social life of survivors of TF GBV is also severely impacted by their abuse, with impacts ranging from safety concerns to reduced contact with significant others, to social isolation.^{xiv}
- The financial impacts of TF GBV include lack of or limited access to finance and online banking; loss of employment; difficulties in securing employment; accrual of debt; payment of fees to remove sexual images from social media and web-based platforms; and the cost of purchasing new or replacement devices.^{xv}
- Costs associated with responding to stalking—which can include legal fees, property damage, childcare costs, moving expenses, changing a phone number or email account, and credit monitoring—are much higher for victims of TF GBV.^{xvi}

Victims can face multiple forms of TF GBV, depending upon the form of technology the abuser decides to misuse—with violence occurring both online and offline.^{xvii} For instance:

Phone

- **Cell Phones:** Abusers often misuse cell phones to track victims' cell phone activity and to identify their locations through the cell phone's GPS.
- **Text Messaging:** Websites permit perpetrators to falsify phone numbers, and many cell phone providers allow text messages to be sent via the internet where cell phone numbers can be faked, allowing multiple harassing and/or threatening messages to be sent.
- **Voice Messages:** Abusers use various methods to leave harassing and threatening messages, including prepaid phone cards or "pay-as-you-go" cell phones to call victims without identifying themselves through caller ID.
- **Caller ID:** Services exist that allow abusers to "spoof" (fake) the phone numbers that are displayed on a caller ID, and even allow abusers to record calls and to fake their voices.

Location and Surveillance

- **Global Position Systems (GPS):** Abusers are increasingly misusing GPS systems to track the real-time precise physical location of victims. Some vehicles come with GPS systems pre-installed, which allow abusers to monitor a survivor's location and to entirely control the survivor's vehicle.
- **Bluetooth Trackers:** Bluetooth trackers such as airtags are being misused by intimate partners and other abusers to stalk their victims. While victims are still in relationships with abusers, or are in close proximity to them, abusers will place the trackers in victims' belongings, or in the belongings of victims' children to stalk and monitor their whereabouts.^{xviii}
- **Hidden Cameras:** Small, wireless cameras can now be placed or purchased pre-installed in a variety of common household items, including smoke detectors, children's toys, and lamps, many of which can be activated remotely.

Email

- **Email:** Anonymous email services allow abusers to send harassing and/or threatening messages to victims, making it more difficult, though not impossible, to identify them and hold them accountable.

Internet and online channels^{xix}

- **Cyber-harassment:** abusers frequently misuse email and social media platforms such as Facebook, Twitter, Instagram, YouTube, Snapchat, etc., to monitor, frighten, and undermine victim's self-esteem or reputation.
- **Cyber-mob attacks:** abusers will collectively attack a target using a barrage of threats, slurs, insults, and other abusive tactics.
- **Deepfakes:** abusers misuse a form of artificial intelligence to manufacture images, audio, and/or video that appear real to make victims appear that they have said or done something they have not.
- **Denial of access:** abusers engage in mass reporting to target a victim's account to get platforms to suspend or shut down it.
- **Doxxing:** abusers can retrieve and publish victims' personal information, including but not limited to: full names, addresses, phone numbers, emails, spouse and children names, and financial details.
- **Hacking & Stalking:** abusers misuse spyware, often marketed for monitoring children's usage, and Remote Access Tools (RATs) to track survivors' computer activity—including emails, instant messages, websites, keystrokes, etc.,—without the victim's knowledge. Abusers can also use hacking to steal data, violate victims' privacy, and infect their devices with viruses.
- **Hate Speech:** abusers often misuse online platforms to attack specific aspects of their victims' identities, such as race, sex, gender identity, religion, sexual orientation, disability, etc.
- **Impersonation:** abusers will often wrongfully obtain and use victims' personal data to create a hoax account to post offensive or inflammatory statements intended to defame, discredit, or instigate further abuse. Abusers can also impersonate someone a victim knows to cause further harm.
- **Misinformation and defamation:** abusers will often spread rumors and slander to discredit or damage their victims' reputation.
- **Swatting:** Abusers will place hoax calls to law enforcement detailing a false threatening event occurring at their victim's residence, with the goal of sending a SWAT team to the victim's address.
- **Video- and image-based abuse:** abusers will engage in sextortion; unsolicited pornography; and unwanted sexual requests, comments, and content to harass and threaten their victims. Abusers also engage in revenge porn by distributing private,

sexually-explicit images/video of their victims without their consent.

- **Violent threats:** abusers will issue threats to inflict pain, injury, damage, or other hostile action against their victims, including death threats, threats of physical violence, and threats of sexual violence.
- **Zoombombing:** Abusers will hijack virtual meetings and disrupt communication by sharing unrelated and unauthorized text, video, or audio.
- **Internet-of-Things / Smart Home Devices^{xx}**
 - Smart home devices such as locks, thermostats, lights, security cameras, doorbells, and speakers: abusers are misusing and exploiting smart-home technology to harass, stalk, monitor, and control their victims.^{xxi}
 - Most smart-home technology is installed by men, and many women do not have applications to control smart home devices installed on their phones, making abuse easier to perpetrate, even once abusers leave the property.^{xxii}

Online violence impacts not only survivors, but society and the economy at large.^{xxiii}

- TF GBV increases the gender divide: almost 9 out of 10 women restrict their online activity in some way to address or avoid TF GBV, limiting their access to employment, education, healthcare, and community.^{xxiv}
- Half of women say that the internet is not a safe place to share thoughts. Women's forced self-censorship means that women's voices and perspectives are underrepresented, reducing diversity in political, economic, and social arenas.^{xxv}

HOW ADVOCATES AND NONPROFITS CAN HELP^{xxvi}

- Understand that technology is not to blame, and that asking survivors to log off, delete, or not use technology will not stop the abuse from happening.
- Believe survivors when they communicate their experiences with technology and gender-based violence. Encourage survivors to trust their instincts.
- Help survivors develop a [technology safety plan](#).
- Help survivors to [document](#) what the abuser is doing and what the survivor is experiencing so that a record of the abusive incidents and behaviors is established. If the survivor chooses to engage with law enforcement, this documentation can be used to help begin an investigation.
- Encourage survivors, for whom it is safe to do so, to download the [Tech Safety App](#) to their mobile device.

- Ensure your organization follows all appropriate confidentiality [protocols](#) to protect survivor safety and privacy.
- Review your [website](#) for technology safety features, such as adding a safety alert header, removing email addresses, and making your website more accessible.
- Review [best practices](#) when offering services to survivors through technology.
- Ensure that any [shelter location](#) remains confidential.

TO LEARN MORE:

- [Technology-Facilitated Gender-Based Violence: An Overview](#)
- [Measuring Technology-Facilitation Gender-Based Violence](#)
- [Measuring the Prevalence of Online Violence Against Women](#)
- [The State of Online Harassment – Pew Research](#)
- [Centre for International Governance Innovation – Gender Section](#)

ⁱ “A Glimpse From the Field: How Abusers Are Misusing Technology.” National Network to End Domestic Violence, 2014.

https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/54e3d1b6e4b08500fcb455a0/1424216502058/NNEDV_Glimpse+From+the+Field+-+2014.pdf.

ⁱⁱ 2022 Online Harassment and Abuse Survey Results Summary - The Hotline, July 2022. https://www.thehotline.org/wp-content/uploads/media/2022/07/2022_Online_Abuse_and_Harassment-Survey.pdf.

ⁱⁱⁱ YWCA acknowledges that there is not a single term to adequately identify the experiences and realities of every all persons affected by technology-facilitated gender-based violence. The terms generally used to identify those affected by this form of violence are many and varied, as are the experiences of those who have been abused, assaulted, and attacked. For purposes of simplicity, we have chosen to use “survivor” when describing individuals who are going through the healing/recovery process and when discussing the short and long-term impacts of TFGBV, and “victim” when discussing the acts of violence associated with TFGBV. For more information, see: <https://upsettingrapeculture.com/survivor-victim/>.

^{iv} Technology-facilitated violence is defined as, “an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated, and amplified in part or fully by the use of information and communication technologies or digital media, 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.” Vaughan, Cathy, Sarah Bergman, Alexandra Robinson, and Stephanie Mikkelson. Rep. *Measuring Technology-Facilitated Gender-Based Violence: A Discussion Paper*. “University of Melbourne – United Nations Population Fund, February 2023. <https://reliefweb.int/report/world/measuring-technology-facilitated-gender-based-violence-discussion-paper>.

^v Vaughan, Cathy, Sarah Bergman, Alexandra Robinson, and Stephanie Mikkelson. Rep. *Measuring Technology-Facilitated Gender-Based Violence: A Discussion Paper*. “University of Melbourne – United Nations Population Fund, February 2023. <https://reliefweb.int/report/world/measuring-technology-facilitated-gender-based-violence-discussion-paper>.

^{vi} Office of Justice Programs, Bureau of Justice Statistics, Rachel E. Morgan, and Jennifer L. Truman, Stalking Victimization, 2019 § (2022). <https://bjs.ojp.gov/content/pub/pdf/sv19.pdf>; Measuring the prevalence of online violence against women, March 1, 2021. <https://onlineviolencewomen.eiu.com/>.

^{vii} Vaughan, Cathy, Sarah Bergman, Alexandra Robinson, and Stephanie Mikkelson. Rep. *Measuring Technology-Facilitated Gender-Based Violence: A Discussion Paper*. “University of Melbourne – United Nations Population Fund, February 2023. <https://reliefweb.int/report/world/measuring-technology-facilitated-gender-based-violence-discussion-paper>.

^{viii} Measuring the prevalence of online violence against women, March 1, 2021. <https://onlineviolencewomen.eiu.com/>.

^{ix} Measuring the prevalence of online violence against women, March 1, 2021. <https://onlineviolencewomen.eiu.com/>.

^x Cyberstalking is defined as using the internet, email, or other electronic means to harass, scare, or threaten someone with physical harm.

^{xi} Office of Justice Programs, Bureau of Justice Statistics, Rachel E. Morgan, and Jennifer L. Truman, Stalking Victimization, 2019 § (2022). <https://bjs.ojp.gov/content/pub/pdf/sv19.pdf>.

^{xii} Nobles, Matt R., Bradford W. Reynolds, Kathleen A. Fox, and Bonnie S. Fisher. “Protection against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization among a National Sample.” *Justice Quarterly* 31, no. 6 (2012): 986–1014. <https://doi.org/10.1080/07418825.2012.723030>.

-
- ^{xiv} Rogers, Michaela, Colleen Fisher, Parveen Ali, Peter Allmark, and Lisa Fontes. "Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review." *Trauma, Violence, & Abuse*, 2022. <https://doi.org/10.1177/15248380221090218>.
- ^{xv} Rogers, Michaela, Colleen Fisher, Parveen Ali, Peter Allmark, and Lisa Fontes. "Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review." *Trauma, Violence, & Abuse*, 2022. <https://doi.org/10.1177/15248380221090218>.
- ^{xvi} Nobles, Matt R., Bradford W. Reynolds, Kathleen A. Fox, and Bonnie S. Fisher. "Protection against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization among a National Sample." *Justice Quarterly* 31, no. 6 (2012): 986–1014. <https://doi.org/10.1080/07418825.2012.723030>.
- ^{xvii} Bowker, Art. (2012). "A Victim Centered Approach to Supervising Internet Harassment Offenders." Perspectives. Retrieved from http://www.appa-net.org/eweb/docs/appa/pubs/Perspectives_2012_Spotlight.pdf.
- ^{xviii} Dunn, Suzie, Tracy Vaillancourt, and Heather Brittain. Rep. *Supporting Safer Digital Spaces: Special Report*. Gentr for International Governance Innovation, 2023. <https://www.cigionline.org/publications/supporting-safer-digital-spaces/>.
- ^{xix} "Defining 'Online Abuse': A Glossary of Terms." Online Harassment Field Manual, June 28, 2023. <https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/>.
- ^{xx} Maria Tanczer, Leonie. "Technology-Facilitated Abuse and the Internet of Things (IOT)." *Technology and Domestic and Family Violence*, 2023, 76–87. <https://doi.org/10.4324/9780429316098-8>.
- ^{xxi} Finegas, Jon. "Domestic Abusers are Exploiting Smart Home Devices." Referred from https://www.huffpost.com/entry/domestic-abusers-are-exploiting-smart-home-devices_n_5b324f53e4b0b5e692f190d3?guccounter=1&guce.
- ^{xxii} Bowles, Nellie. (June 23, 2018). "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse." Retrieved from <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>.
- ^{xxiii} Measuring the prevalence of online violence against women, March 1, 2021. <https://onlineviolencewomen.eiu.com/>.
- ^{xxiv} Measuring the prevalence of online violence against women, March 1, 2021. <https://onlineviolencewomen.eiu.com/>.
- ^{xxv} Measuring the prevalence of online violence against women, March 1, 2021. <https://onlineviolencewomen.eiu.com/>.
- ^{xxvi} Special thanks to the National Network to End Domestic Violence Safety Net Project for these tips, tools, and suggestions: <https://www.techsafety.org/>.