# Family Violence & Family Law Brief

## Tech-Facilitated Violence: An Introduction

Issue #14 | March, *2022*

ALLIANCE OF CANADIAN RESEARCH CENTRES
ON GENDER-BASED VIOLENCE

This Brief was prepared by RESOLVE Manitoba (Research and Education for Solutions to Violence and Abuse), a member of the Alliance of Canadian Research Centres on Gender-Based Violence.

RESOLVE Manitoba is based at the University of Manitoba, Winnipeg, Manitoba, Canada, on original lands of Anishinaabeg, Cree, Oji-Cree, Dakota, and Dene peoples, and on the homeland of the Métis Nation.

---

## Suggested Citation

Hoffart, R. & Kardashevskaya, M. (2022). Tech-Facilitated Violence: An Introduction. Family Violence & Family Law Brief (14). Winnipeg, Manitoba: RESOLVE (Research and Education for Solutions to Violence and Abuse)

## Design

Diana Corredor, Communications Coordinator at the Centre for Research & Education on Violence Against Women & Children & Patricia Karacsony, Digital Communications Specialist at RESOLVE

## Translation

Sylvie Rodrigue

## Share Your Feedback on This Brief

Click the following link to share feedback about this Brief or suggestions about future resources:

https://uwo.eu.qualtrics.com/jfe/form/SV_bayzVPBefHsfER8

## Join us

Email us if you would like to receive information about future resources and webinars: RESOLVE@umanitoba.ca

***The brief is based on the presentation of Jane Bailey and Suzie Dunn** "Tech-facilitated violence: an introduction" held on November 24, 2021 by RESOLVE Manitoba. The webinar can be retrieved from: https://www.youtube.com/watch?v=GXlL0qNflWI*

Public Health Agency of Canada | Agence de la santé publique du Canada

# Tech Facilitated Violence: An Introduction

## Introduction

The world has been experiencing a greater accessibility of such technologies as the internet, smartphones, various software and applications, artificial intelligence (AI), and the omnipresence of social media. Additionally, there have been higher levels of use and dependence on these technologies.

Technology offers new ways of addressing gender-based violence, for example, through social media campaigns that target diverse audiences or smartphone applications that can help intimate partner violence (IPV) survivors access support services (Emezue, 2020). These new technologies, however, also pose significant challenges to addressing gender-based violence. Thus, in 2014, the BC Society of Transition Houses (BCSTH) conducted a survey among service providers regarding the intersection of violence and technology, finding that:

- 98% of service providers had worked with women and girls who were threatened via technology
- 72% supported women and girls whose email and social media accounts had been hacked
- 69% supported women and girls whose perpetrator impersonated them in an online space (e.g., social media page, dating website)
- 89% of service providers expressed a need for more information about tech-facilitated violence

This short brief explores the issue of facilitated violence and is based on the webinar, *Tech-Facilitated Violence: An Introduction* hosted by RESOLVE at the University of Manitoba with keynote speakers Jane Bailey (University of Ottawa, The eQuality Project) and Suzie Dunn (Dalhousie University, The eQuality Project). The brief defines basic terms and definitions, provides an overview of tech-facilitated violence (TFV), discusses tech-facilitated gender-based violence (TFGBV), examines the issue of tech-facilitated IPV, and provides practical tips for safety planning along with a list of useful resources.

## Terms & Definitions

There are many forms of tech-facilitated violence that involve multiple forms of technology and myriad strategies of abuse. Dunn (2020) groups tech-facilitated violence into four categories: harassment, image-based sexual abuse, privacy invasions, and impersonation:

1. *Harassment*: includes any form of unwanted digital communication. It is the most common and well-known form of tech-facilitated violence and can include any of the following.
    - Unwanted Messages: can include harmful messages from a current or former partner, unwanted communication from acquaintances, and/or receiving unsolicited explicit sexual images that were sent with the intention of disturbing the recipient and causing them harm.

- Networked Harassment: involves groups of people (networks) who have come together to target a single individual and/or type of individual with the intention of causing them harm.
- Defamation: occurs when people or groups share false information online that is damaging to the reputation of a person and/or a group of people. Defamation can also be related to fake websites and impersonation, both of which are explored in greater detail below.
- Threats: are another commonly recognized form of tech-facilitated violence that can include death threats and threats of sexual violence that are normalized in digital space. In many instances, these threats are targeted at people based on their social location, and often aimed at women and members of 2SLGBTQ+ communities.
- Hate Speech: is derogatory communication shared online which is directed toward a person or group on the basis of characteristics related to race, class, gender, sexual orientation, and/or other similar categories. In online spaces it is often directed toward women and members of racialized groups.

2. *Image-Based Sexual Abuse:* involves the distribution of intimate images. This form of abuse is relatively common, can take many different forms, including what is often referred to as non-consensual distribution of intimate images.
   - Creepshots/Voyeurism: occur when someone uses a hidden device (e.g., camera, video recorder) to take secretive images or videos of someone in settings where that person could reasonably expect privacy.
   - Livestreaming/Documenting Assaults: involves recording/digitally documenting and distributing assaults/sexual assaults. It can be understood as a strategy to amplify the violence and create another level of abuse.
   - Sextortion: occurs when an individual uses intimate image of someone (consensual or non-consensual) to coerce their victim into staying in an unwanted situation. It can arise within the context of violent relationships and/or human trafficking.
   - Deepfakes: involve use of artificial intelligence technology to swap the faces of people in videos or other pictures. It often involves inserting someone's image into sexual videos without their consent. They are a more technologically-advanced form of image-based abuse.

3. *Privacy Invasions:* are a form of tech-facilitated violence where individuals expose personal information about another person online without their consent.
   - Public Disclosure of Private Information: publishing private and/or embarrassing information and pictures online without an individual's consent.
   - Doxing: finding someone's private information (e.g., home address, phone number) and publishing it online without their consent. This information is then used to intimidate the victim.
   - Stalking and Monitoring: can involve complex forms of technology (Stalkerware) which are installed on the victim's devices and used to monitor their activities. Stalking and monitoring can also involve more basic apps such as Find My iPhone. This form of abuse can also be perpetrated in instances where an abuser demands access to their victim's devices.

4. *Impersonation:* using technology involves damaging the victim's reputation by impersonating them on social media platforms, dating profiles, websites, or other online spaces, which can be particularly harmful because of the increasing importance and impact of people's online reputations.
    - Fake Websites: involve an individual creating a fake website about their victims in an effort to damage their reputation. It can include posting information about the victim that is personal, private, harmful, or embarrassing and spreading lies.
    - Fake Dating Profiles: involve an individual creating a fake dating profile for their victim without their consent and falsely indicating that that person is available for sexual activities or rape fantasies.
    - Spoofing: involves sending "fake" text messages or emails so that it looks like it is coming from the victim's phone or email accounts when it is not. An individual may spoof their victim to get them into trouble for something they haven't said or done. Proving that spoofing has occurred is difficult because it appears as though the communication has originated from the victim's accounts.

## Tech-Facilitated Gender-Based Violence

Gender-based violence (GBV) is violence that is directed against an individual or group of individuals based on their gender identity, gender expression, or perceived gender. It can happen to individuals of any gender identity; however, GBV often targets women, girls, and gender-diverse people, particularly those from marginalized groups (Government of Canada, 2021). GBV is a significant social issue that has traditionally been understood within the context of offline interactions. However, more recently with the accessibility of digital technologies and the growing centrality of online interactions, there are new forms of violence that are facilitated by technology. Tech-facilitated gender-based violence (TFGBV) can be understood as a component of the broader continuum of gender-based violence (Khoo, 2021).

TFGBV is a term used to refer to an "action by one or more people that harms others based on their sexual or gender identity or by enforcing harmful gender norms" and that is "carried out using the internet and/or mobile technology and includes stalking, bullying, sexual harassment, defamation, hate speech and exploitation" (Hinson et al., 2018, p. 1). TFGBV has also been referred to as cyberbullying, trolling, online abuse, cyber violence, digital harassment, tech-facilitated coercive control, symbolic violence, and representational violence (Bailey & Dunn, 2021). TFGBV is a gendered social issue because of the frequent targeting of women, girls, gender-diverse and gender non-conforming people. This form of violence also intersects with other forms of discrimination, including those related to race, class, disability, and sexual orientation (Dunn, 2021).

Technology such as Global Positioning System (GPS) trackers, social media platforms, smartphone apps, and Internet of Things devices (e.g., smart locks, smart speakers) have been used in the perpetration of TFGBV (Slupska & Tanczer, 2021). There are also new forms of violence that have emerged with the increased accessibility and enhanced prominence of technologies. Doxing, impersonation, deepfakes, voyeurism, and spoofing are just a few examples of tech-facilitated violence that have been used to intimidate, threaten, undermine, harass, and control victims (Bailey & Dunn, 2021; Dunn, 2020).

Data from the 2014 General Social Survey (GSS) illustrates the gendered nature of cyberstalking and cyberbullying in Canadian society. Just under one-fifth (17%) of young Canadians aged 15 to 29 years reported experiencing cyberbullying or cyberstalking. Youth (particularly those who have previously experienced violence or discrimination), gender-diverse individuals, and women were more likely to report experiencing these forms of TFV (Burlock & Hudon, 2018; Hango, 2016). Activist girls and young women who talk about gender equality and other social justice issues are likely to experience tech-facilitated violence at a very young age, which can have a negative impact on overall social development and gender justice (Bailey & Dunn, 2021).

TFGBV is also an intersectional issue with disproportionately negative impacts on women in leadership roles (e.g., politicians, activists, human rights defenders), as well as women from Black, Indigenous and other racialized communities, those who are IPV victims/survivors, those who are members of 2SLGBTQ+ communities, those living with disabilities and those who are young.

## Impacts of Tech-Facilitated Gender-Based Violence

TFGBV can have devastating impacts on victims/survivors, particularly in relation to their social standing because it creates a permanent digital record, can be spread worldwide, and is not easily deleted (Šimonović, 2018). It can lead to reputational harm, negative self-perception, community-based shaming, mental health problems (including PTSD, suicidal ideation, anxiety, etc.) and financial hardships (e.g. loss of employment). TFGBV and its negative effects are not limited to the online world. It can be an extension of offline violence that survivors experience, and its effects can permeate survivors' all aspects of survivors' lives (Bailey & Dunn, 2021; Dunn, 2020).

At a systemic level, TFGBV silences women and other marginalized groups reducing their "participation in digital spaces and leadership roles" exacerbating the social, economic, and political disempowerment of women, girls, and other marginalized groups (Dunn, 2020, p. 22). Khoo (2021) argues that this can have a dire effect on the quality of democracy.

Despite growing awareness of the impacts of TFGBV, a need for nuanced understandings of the negative consequences for survivors and development of possible solutions toward the issue still persists. Violence that occurs in digital spaces is often misunderstood, and in some instances it may be perceived as minor or insignificant. Consequently, authorities may fail to recognize the problem and/or take action toward the issue. In many cases, the proposed solution toward tech-facilitated violence is for the victim/survivor to limit their online activity, self-censor, and/or disconnect from technology (Dunn, 2021). However, self-censorship and disconnection are not viable solutions due to the importance of one's online presence in today's world. Further, in some cases victims/survivors' experiences are not captured within existing criminal law (Khoo, 2021).

## Finding a Way Forward

Meaningfully addressing TFGBV and supporting survivors requires a multi-pronged approach that might include legal, educational, and technology-based solutions. Many digital platforms (e.g., Facebook, Twitter, YouTube) have developed community policies that prohibit hate speech, violence incitement, pornography, and nudity. Many of these platforms also have tools that enable flagging, reporting, fact-checking, and moderation of harmful content. These policies and tools, however, have not proven particularly effective for a variety of reasons. For example, in some instances the business model of these companies makes it profitable to leave up harmful content, making them reluctant to implement strategies for meaningfully addressing TFGBV (Khoo, 2021). Khoo (2021) argues that there should be policy changes in Canada to address TFGBV on these platforms, such as an establishment of a centralized expert regulator for TFGBV and a process that enables quick and efficient removal of certain harmful content without a court order. Policy solutions, however, must incorporate an intersectional analysis and focus on substantive equality in order to ensure that they do not end up harming the very people they are meant to serve and support. Khoo (2021) also argues that more funding is needed to support research aimed at understanding the complexities of TFGBV and to develop enhanced services for victims/survivors.

## Tech-Facilitated Intimate Partner Violence

As mentioned above, TFVGB is often employed in abusive relationships with perpetrators using a multitude of tools to control their victims (Laxton, 2014). The power and control dynamic associated with IPV is particularly significant when it is carried out through technology because abusers are able to monitor and control their victim's actions, creating a sense of omnipresence (Bailey & Dunn, 2021). Tech-facilitated intimate partner violence (TFIPV) can be a particularly debilitating strategy for abuse due to its constant and pervasive nature.

Research has identified (Freed et al., 2017; Borrajo et al., 2015) several forms of TFIPV commonly seen in violent relationships, including:

- online stalking and harassment
- sending insults and threats over social media platforms, email, and text
- sharing private/embarrassing information about the victim in online spaces
- using technology (e.g., Find My iPhone, Stalkerware) to monitor the victim's devices and online activity

Certain aspects of TFIPV put abusers in uniquely powerful positions. For example, in many instances, the abuser has access to the victim's devices and online accounts. Coercive strategies are often employed by abusers to pressure their victims into sharing this information. This accessibility makes it easy to make changes to the victim's social media accounts, install tracking software, and/or manipulate their information in another way. Abusers may be able to figure out the victim's device and social media passwords because they have knowledge of that person's life circumstances, enabling them to correctly answer the security questions (Dunn, 2020).

The complexities of TFV present significant challenges to the safety planning process. Accordingly, safety planning strategies must take into account the unique power and control dynamic that exists within the context TFV. Education and awareness around the issue combined with improved corporate and police responsibility and accountability, tech literacy and online safety are important starting points toward addressing the issue.

## Safety Planning – Tech-Facilitated Intimate Partner Violence

The following safety planning tips were adapted from resources produced by the British Columbia Society of Transition Houses (2022) and HackBlossom (2022).

1. ***Look for patterns.*** Think about the ways that technology may be used to harass, monitor, or stalk. Identify abuse patterns and narrow down the forms of technology used to perpetrate the abuse, and use this information to develop a safety plan. Document the incidents and report them to authorities.

2. ***Think about using a safer device.*** If you think that someone is monitoring your computer, smart phone, tablet, consider using a different device that the abuser has not had physical and/or remote access to.

3. ***Change your password and usernames.*** Review the privacy settings on your devices. Ensure that device-to-device access is disabled and that there aren't other accounts linked to yours. Use strong passwords to reduce the possibility of your accounts being hacked. Consider using two-step verification for your accounts.

4. ***Monitor data usage levels.*** Spikes in data usage can indicate that monitoring software is in use.

5. ***Protect your location.*** Review smartphone settings, apps, and accounts to identify whether your location sharing is turned on. Contact your wireless provider and roadside assistance/safe drive services to determine if location tracking is enabled on your accounts.

6. ***Protect your address and limit the information you give out about yourself.*** Limit the number of people with which you share your personal information. Avoid sharing personal and contact information on social media platforms.

7. ***Get more information.*** Connect with local resource centres, shelters, and law enforcement agencies for assistance. Additional information and safety planning resources can be found in the *Resources* section of this brief.

# Tech-Facilitated Intimate Partner Violence and Family Court Issues

The recent amendments to the *Divorce Act* include a comprehensive definition of family violence that encapsulates a wide range of abusive behaviours, including stalking and harassment. Repeatedly calling, emailing, or texting a victim; tracking a victim's activities using apps or specialized software (e.g., Stalkerware); and monitoring the victim through social media platforms are examples of stalking and harassment facilitated through the use of technology (Department of Justice, 2022). TFIPV is a significant issue within the family court system and has important implications for survivors and their children. A recent review of family law cases found that technology (i.e., email, texting, social media interactions) played a central role in the family court process, specifically in relation to communication regarding custody, access, and exchange (Koshan et al., 2020). Within the context of the COVID-19 pandemic, technology has become increasingly important and serves the primary mechanism to facilitate conversations related to shifting access/exchange arrangements and the well-being of the child(ren) during the pandemic.

Despite the numerous risks associated with TFIPV for survivors and their children, there is a lack of understanding regarding the nature and context of the issue. Consequently, the misconceptions surrounding the issue present significant challenges for survivors navigating the family court system in instances of TFIPV.

A 2022 study found that mothers and children are often co-victims of TFIPV, despite the fact that tech-facilitated communication is viewed by the family court as a safer alternative to face-to-face communication in relationships involving IPV (Dragiewicz et al., 2022). Court-mandated requirements regarding communication about the child (e.g., email updates, making access/exchange arrangement via text message) may present unsafe situations for mothers by putting them in direct contact with their abuser. Children may cross-carry digital devices between their parents' homes, providing an opportunity for the abuser to install various kinds of software and track the location of their victim (Dragiewicz et al., 2022). TFIPV can also negatively impact parenting in instances where parents limit their children's online interactions due to fears of TFIPV.

# Resources

This section highlights several online resources related to tech-facilitated violence, digital hygiene, and safety planning.

### BC Society of Transition Houses

Website: https://bcsth.ca/techsafetytoolkit/

The BC Society of Transition Houses has developed an online *Technology Safety and Privacy Toolkit* that teaches individuals how to increase technological safety and privacy. The toolkit includes a section on general technology safety, devices and hardware technology safety tips, safety and security when using smart appliances, online safety and privacy tips, and potential legal remedies for tech-facilitated violence.

### HackBlossom

Website: https://hackblossom.org/domestic-violence/

HackBlossom is an initiative that aims to equip IPV survivors with an understanding of tech-facilitated threats and protection strategies.

### Clinic to End Tech Abuse

Website: https://www.ceta.tech.cornell.edu/resources
This is an online guide that provides information about how to disconnect from abusive partners/ex-partners, check appliances for spyware and other hidden apps, and making online accounts secure and safe (e.g., Gmail, Hotmail, Facebook and other social media).

### YWCA Project Shift

Website: http://projectshift.ca
The Project Shift website provides several guides related to technology-related safety. Examples include a guide with tips and tools for supporting young women and girls who experience cyberviolence; and a guide on sexual image-based abuse that explains the nature of the issue, legal considerations, and available resources/supports.

### Feminist Frequency

Website: https://onlinesafety.feministfrequency.com/en/#preventing-doxxing
The Feminist Frequency is an online guide about online harassment and doxing.

### CrashOverride

Website: http://www.crashoverridenetwork.com
CrashOverride is a project created to promote online safety and prevent online violence. The website features a resource center with several useful guides for understanding tech-facilitated violence.

### Toxic Hush Action Kit

https://www.informedopinionstoxichushkit.org/
The Toxic Hush Action Kit aims to provide support and resources for survivors of tech-facilitated violence and online abuse. The website also includes information for allies and those supporting survivors of tech-facilitated violence.

## *Resources - Social Media Safety and Online Presence Removal*

### HeartMob

Website: https://iheartmob.org/resources/safety_guides
HeartMob developed a social media safety guide for various platforms, including Facebook, Instagram, Twitter, Reddit, Tumblr, Tiktok, Zoom, and Youtube.

### Cyber Civil Rights Initiative

Website: www.cybercivilrights.org/online-removal/
The Cyber Civil Rights Initiative website features a guide for removing intimate images from social media platforms.

### Intel Techniques

Website: https://inteltechniques.com/data/workbook.pdf
The Intel Techniques website includes a workbook that lists the steps for removing one's personal data that is available online.

## *Resources – Identifying & Removing Spyware*

### Coalition Against Stalkerware

Website: https://stopstalkerware.org/
The Coalition Against Stalkerware is concerned with the widespread use of Stalkerware and aims to combat its use. Their website contains short guides for tech companies, media, and survivors.

## *Canada-Based Research Projects on Tech-Facilitated Violence*

### The CitizenLab

CitizenLab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto. Their research focuses on digital espionage, emerging technologies, and the impact on freedom of expression, privacy, security, and surveillance.

Their research on technology-facilitated violence produced two relevant reports on Stalkerware available here: https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/

### The eQualityProject

The eQuality Project is based at the University of Ottawa. Their research focuses better understanding young people's experiences with privacy and equality in a digitally networked environment, focusing not just on individual acts of TFV, but also the ways in which corporate practices set young people up for conflict and harassment.

Policy papers are available here: https://www.equalityproject.ca/policy/policy-papers/
Research publications are available here: https://www.equalityproject.ca/research/research-publications/

### Women's Legal Education and Action Fund (LEAF)

LEAF's work on tech-facilitated violence brings together feminist lawyers and academics to study and imagine possible legal responses to TFGBV. Most recently, they published a report *Deplatforming Misogyny* authored by Cynthia Khoo that looks at possible legal solutions to TFGBV on digital platforms.

Project materials can be accessed here: https://www.leaf.ca/project/tfv/

# References


Bailey, J., & Dunn, S. (2021, November 24). *Tech-facilitated violence: an introduction* [webinar]. RESOLVE. Retrieved from: https://www.youtube.com/watch?v=GXlL0qNflWI

BC Society of Transition Houses. (2014). *Technology misuse & violence against women: Survey* [infographic]. Retrieved from: https://bcsth.ca/wp-content/uploads/2015/12/SNC_TechMisuse-Infograph2013-English.pdf

BC Association of Transition Houses. (2022). *The technology safety and privacy toolkit*. Retrieved from: https://bcsth.ca/techsafetytoolkit/

Borrajo, E., Gámez-Gaudix, M., Pereda, N., & Calvete, E. (2015). The development and validation of the cyber dating abuse questionnaire among young couples. *Computers in Human Behavior, 48,* 358–65.

Burlock, A., & Hudon, T. (2018). *Women and men who experienced cyberstalking in Canada.* Statistics Canada. Retrieved from https://www150.statcan.gc.ca/n1/pub/75-006-x/2018001/article/54973-eng.htm

Department of Justice. (2022). *Divorce and family violence* [fact sheet]. Retrieved from: https://www.justice.gc.ca/eng/fl-df/fsdfv-fidvf.html

Dragiewicz, M., Woodlock, D., Salter, M., Harris, B. (2022). "What's mum's password?": Australian mother's perceptions of children's involvement in technology-facilitated coercive Control. *Journal of Family Violence*, *37*, 137-149. https://doi.org/10.1007/s10896-021-00283-4

Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview* (Supporting a Safer Internet Paper No. 1.). Centre for International Governance Innovation (CIGI). Retrieved from: https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/

Emezue, Chuka. (2020). Digital or digitally delivered responses to domestic and intimate partner violence during COVID-19. *JMIR Public Health Surveillance*, *6* (3), 1-9. https://doi.org/10.2196/19831

eQuality Project (2020). Technologically-facilitated violence: Criminal harassment case law. Retrieved from http://www.equalityproject.ca/wp-content/uploads/2020/07/TFVAW-Criminal-Harassment-3-July-2020.pdf

Freed, D., Palmer, J., Minchala, D.E., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technology and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction, 1* (46), 1-22.

Government of Canada. (2021). *What is gender-based violence?* Retrieved from https://women-gender-equality.canada.ca/en/gender-based-violence-knowledge-centre/about-gender-based-violence.html

HackBlossom. (2022). *Defense strategies.* Retrieved from: https://hackblossom.org/domestic-violence/#defense

Hango, D. (2016). *Cyberbullying and cyberstalking among internet users aged 15 to 29 in Canada.* Statistics Canada. Retrieved from https://www150.statcan.gc.ca/n1/pub/75-006-x/2016001/article/14693-eng.htm

Hinson, L., Mueller, J., O'Brien-Milne, L., & Wandera, N. (2018). *Technology-facilitated gender-based violence: What is it, and how do we measure it?* Washington, DC: International Center for Research on Women

Khoo, C. (2021). *Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence.* Toronto, ON: Women's Legal Education and Action Fund (LEAF).

Koshan, J., Mosher, J., Wiegers, W. (July 13, 2020). COVID-19, domestic violence, and technology-facilitated abuse. *ABlawg*. Retrieved from: http://ablawg.ca/wp-content/uploads/2020/07/Blog_JK_JM_WW_COVID19_Surveillance.pdf

Laxton, C. (2014). *Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking.* Bristol, UK: Women's Aid Federation of England. Retrieved from https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf

Šimonović, D. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.* United Nations. Retrieved from https://digitallibrary.un.org/record/1641160?ln=en

Slupska, J. and Tanczer, L.M. (2021). Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things (pp. 663-688). In Bailey, J., Flynn, A. and Henry, N. (Eds.) The emerald international handbook of technology-facilitated Violence and Abuse. Emerald Publishing Limited: Bingley, UK. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/978-1-83982-848-520211049/full/html