Centre for International
Governance Innovation

Special Report

Supporting Safer Digital Spaces

Suzie Dunn, Tracy Vaillancourt
and Heather Brittain

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Manager, Government Affairs and Partnerships Liliana Araujo
Research Associate Kailee Hilt
Senior Publications Editor Jennifer Goyder
Publications Editor Susan Bubak
Graphic Designer Abhilasha Dewan

For publications enquiries, please contact publications@cigionline.org.

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Project

Supporting a Safer Internet is a multi-year research project, in partnership with the International Development Research Centre (IDRC). This project explores the prevalence and impacts of technology-facilitated gender-based violence (TFGBV) experienced by women, transgender, gender non-conforming and gender-diverse people, as well as technology-facilitated violence (TFV) against LGBTQ+ individuals.

As part of the project, an international survey was conducted by Ipsos on behalf of the Centre for International Governance Innovation (CIGI). The survey results provide valuable insight on people's experiences with online harms in 18 different countries, with a specific focus on the Global South. From cyberstalking, impersonation and the non-consensual distribution of intimate images, to organized networked harassment, TFGBV causes serious harm and silences the voices of women, gender-diverse people and LGBTQ+ individuals in digital spaces. Fear of TFGBV leads to digital exclusion and propagates systemic inequalities. To address these emerging challenges, the survey results, papers and the *Supporting Safer Digital Spaces* report from this project aim to inform policy recommendations and navigate shared governance issues that are integral to designing responses to TFGBV — whether that be through the regulation of online social media platforms, educational programming or legal recourse.

This project was assisted by an expert advisory committee made up of Chenai Chair (Mozilla Foundation), Jan Moolman (Association for Progressive Communication), Anja Kovacs (independent researcher and consultant, previously at Internet Democracy Project), María Paz Canales (Global Partners Digital, previously at Derechos Digitales) and Ruhyia Seward (IDRC).

In addition to this report and an annotated bibliography, the following papers have been published as part of this project:

- Suzie Dunn, *Technology-Facilitated Gender-Based Violence: An Overview*, Supporting a Safer Internet Paper No. 1 (2020)
- Michelle Bordachar, Nonhlanhla Chanza, Kailee Hilt, J. Carlos Lara, Emma Monteiro and Grace Mutung'u, *Non-Consensual Intimate Image Distribution: The Legal Landscape in Kenya, Chile and South Africa*, Supporting a Safer Internet Paper No. 2 (2021)
- Florencia Goldman, *Non-binary TikTokers in Latin America: Sharing Debates and Circumventing Censorship*, Supporting a Safer Internet Paper No. 3 (2021)

Publications, multimedia, country data reports and opinions related to the project can be found on CIGI's website: **www.cigionline.org/activities/supporting-safer-internet/.**

Foreword

Various forms of digital technology are being used to inflict significant harms online. This is a pervasive issue in online interactions, in particular with regard to technology-facilitated gender-based violence (TFGBV) and technology-facilitated violence (TFV) against LGBTQ+ people. This modern form of violence perpetuates gender inequality and discrimination against LGBTQ+ people and has significant impacts on its targets, including silencing women's and LGBTQ+ persons' voices online.

On the occasion of International Women's Day (March 8) in 2020, the Centre for International Governance Innovation (CIGI) announced that it had received a grant from the International Development Research Centre (IDRC) for a project titled Supporting a Safer Internet. The project was officially launched with the Honourable Karina Gould, then Canada's minister of international development, who said: "This is an important project to arm governments, NGOs and private sectors including social media entities with this data to design effective responses for a safer online world."

The project aimed to conduct ground-breaking research by undertaking a major international survey of people's experiences with online harms with a specific focus on countries in the Global South. The research aimed to provide concrete evidence of those experiences to inform and influence policy. The objective was to use this first-of-its-kind research to create policy and legal recommendations to better protect vulnerable and marginalized populations, in particular women and LGBTQ+ people, from the insidiousness of identity-based online harms.

The project achieved three objectives: conducting an international survey on online harms, convening experts and scholars to prioritize policy-related inputs, and producing analysis of TFGBV in the Global South. The survey was conducted in 18 countries and key findings include the international prevalence of online harms, as well as the impacts on the mental health, safety and freedom of expression of women and LGBTQ+ people.

The project has published several research papers and opinion pieces on TFGBV and its impact on women and LGBTQ+ individuals globally. The papers discuss the various forms of online harm and their harmful effects on victims/survivors.

CIGI has also hosted virtual events and discussions to explore the issue and propose solutions. This CIGI special report summarizes the quantitative data collected on people's experiences with and opinions of online harms, with a particular focus on the ways that a person's gender identity, gender expression and/or sexual orientation impact their experiences with online harms, and provides policy recommendations for governments, technology companies, academics, researchers and civil society organizations.

The data for each country is presented with highlights in an individual "data report," organized by survey question to make it easy to identify the key findings. The SPSS file of data is also being made publicly available to inspire and inform current and future research. The aim is to promote transparency and accountability in research and contribute to a safer and more equitable online environment for vulnerable and marginalized populations.

I would like to express gratitude to everyone who contributed to the development of this special report. First and foremost, the project owes a tremendous debt of gratitude to Suzie Dunn, the primary author of this report. Her extensive knowledge and expertise on TFGBV have been invaluable in helping guide this project and in authoring this comprehensive report.

Liliana Araujo showed exceptional ability in managing the project and collaborating with internal and external stakeholders. Her leadership and guidance have been critical in bringing this report to fruition.

I extend CIGI's appreciation to the members of the project steering committee, María Paz Canales, Chenai Chair, Anja Kovacs and Jan Moolman, for their valuable insights and contributions to this report, and to Tracy Vaillancourt and Heather Brittain for their double-hatted role in authoring the report with Suzie and for their advice and counsel on research and statistical methodology along the way. The steering committee's expertise in the fields of human rights, technology and gender-based violence online was instrumental in shaping the report's recommendations and conclusions.

Additional external experts provided insightful commentary on sections of earlier drafts of this report, including members of the Association for Progressive Communications: Nicola Henry, Tigist Hussen, Rosel Kim and Molly Reynolds.

The Ipsos team, Sean Simpson and Sanyam Sethi, contributed to the design, execution, analysis and delivery of the quantitative research exercises. Their expertise and dedication have been invaluable.

I am also grateful to the rest of the CIGI team, Anne Blayney, Susan Bubak, Sara Daas, Michael Den Tandt, Abhilasha Dewan, Dianna English, Niyosha Freydooni, Jennifer Goyder, Andrea Harding, Trevor Hunsberger, Tim Lewis, Rebecca MacIntyre, Rohinton P. Medhora, Emma Monteiro, Kate Pearce, Paul Samson, Lynn Schellenberg, Spencer Tripp, Som Tsoi, Claire van Nierop, Yang Wang and John Xu, for their support and collaboration throughout the project. A special thank you goes to Kailee Hilt, who played an essential role in this project by writing the annotated bibliography and by being a key figure in the creation of each of the country data reports.

Our colleagues at Global Affairs Canada have been instrumental in providing advice and support throughout this process.

This report would not have been possible without the contributions of all these individuals. I am deeply appreciative of their hard work and dedication.

TFGBV is a complex issue that requires a multifaceted approach that involves governments, civil society organizations and technology companies. Social media companies need to be more responsive to the needs of people experiencing violence and provide meaningful support for those abused on their platforms. Front-line anti-violence organizations require increased resources and support to provide adequate intervention strategies, while governments should ensure that there are practical and accessible avenues for those targeted by TFGBV to get the support they need and to hold perpetrators accountable for their actions.

Finally, I would like to express my sincere gratitude to IDRC for its partnership and support throughout this project. I am particularly grateful to Ruhiya Seward, whose idea sparked the project and who has been a vital driving force behind its success. Her insights, guidance and dedication have been critical to the project's progress and impact. I am honoured to have worked with such a committed and inspiring partner and look forward to continuing our collaboration with IDRC on future initiatives.

I hope that this report will contribute to the ongoing efforts to address TFGBV and make the internet a safer space for all.

Aaron Shull
Managing Director and General Counsel, CIGI

Expert Advisory Committee

This project would not be possible without the decades of work done by feminist, LGBTQ+ advocates, digital rights groups and anti-violence organizations that brought this issue to light. Civil society organizations are often at the forefront of intersectional feminist policy making and public education on gender-based violence and violence against LGBTQ+ people. It can take years of dedicated work by these organizations before governments react to them, social norms begin to change, and laws and resources are developed. This remains true with TFGBV and TFV against LGBTQ+ people, and the authors are indebted to that history and the work done before this time.

Although this report will not be able to acknowledge the wide array of organizations and researchers that have contributed to the history of TFGBV research and advocacy, this section will highlight the work of the project's expert advisory committee and organizations they have been a part of in addressing TFGBV and TFV against LGBTQ+ people. Special thanks must be given to the members of the expert advisory committee — their expertise was foundational to the development of the survey and is relied on extensively in this report.

Association for Progressive Communications

The Association for Progressive Communications (APC)[1] has been a significant global leader in research, education and advocacy on TFGBV and TFV against LGBTQ+ people. It has implemented various projects, including GenderIT,[2] Take Back the Tech,[3] Feminist Principles of the Internet[4] and the Feminist Internet Research Network.[5] These projects were some of the first in the world to tackle this issue. This organization began its work on TFGBV in the early 2000s. In 2005, it published the paper "Cultivating Violence through Technology? Exploring the Connections between Information Communication Technologies (ICT) and Violence Against Women (VAW)."[6] Jan Moolman, who worked for APC's Women's Rights Programme as a senior project coordinator on online gender-based violence (OGBV) and currently represents APC on the steering committee of the advisory group of the Global Partnership for Action on Gender-Based Online Harassment and Abuse, attended her first International Governance Forum in 2009, where she noted the lack of global and feminist perspectives on internet governance issues.[7] APC was committed to bringing these perspectives to the field of information technology. In 2011, APC published the paper "Voices from Digital Spaces: Technology Related Violence against Women," which outlined this issue and the role of various stakeholders in responding to it.[8] Since that time, APC has published numerous studies, reports and articles addressing TFGBV worldwide.[9] There is now a robust collection of researchers, policy makers, advocates and educators working on this topic around the world.

Take Back the Tech

Take Back the Tech was established by APC in 2006.[10] It shares information on how people can use technology to end gender-based violence, in particular TFGBV. It has organized various campaigns, often around the 16 Days of Activism Against Gender-based Violence. Previous and current campaigns include the 2013 #FBRape campaign that brought attention to Facebook groups that glorified violence against women and girls and Facebook's lack of response to this harmful content,[11] the "What are You Doing about Technology-related Violence against Women?" campaign,[12] and its most recent campaign "Whose

1 See www.apc.org/.

2 See https://genderit.org/.

3 See https://takebackthetech.net/.

4 See https://feministinternet.org/.

5 See https://firn.genderit.org/.

6 See Kee (2005).

7 See Kovacs et al. (2012).

8 See Fascendini and Fialová (2011).

9 See www.apc.org/en/our-work.

10 See https://takebackthetech.net/about.

11 See www.apc.org/en/news/fbrape-campaign-and-necessary-debate.

12 See https://genderit.org/editorial/editorial-recognition-online-gbv-international-law-highs-and-lows.

Streets? Ours! Witness Silencing. Occupy. Create," which focused on the history of women and technology and denouncing TFGBV.[13] Its work brings much-needed education to the world about TFGBV.

GenderIT

GenderIT was established in 2006 and is a communication platform that addresses women's rights surrounding the internet. It primarily focuses its research on Africa, Asia, Latin America, Arabic-speaking countries and Eastern Europe.[14] It has explored TFGBV in Argentina,[15] Bangladesh,[16] Brazil,[17] Egypt,[18] India,[19] Malaysia,[20] Mexico,[21] the United States[22] and Palestine,[23] among other countries.[24] Its research examines the experiences of women and people of diverse gender expressions including gender non-conforming, gender queer, transgender, non-binary, intersex people and other gender-marginalized people. In this work, GenderIT explored various legal, technological and social remedies available to gender minorities experiencing TFGBV, how intersecting marginalities influenced the impact of TFGBV, and the silencing effect TFGBV had on women and gender-diverse people.[25] Its work often engages in qualitative research to share the stories of women and gender-diverse people who have experienced TFGBV in various countries, focusing on intersecting factors such as sexual orientation, race, caste and other marginalizing social positions.

13 See https://takebackthetech.net/blog/whose-streets-ours-witness-silencing-occupy-create-25-nov-10-dec.

14 See https://genderit.org/about.

15 See Alcaraz (2017).

16 See Akter (2018).

17 See Valente (2018).

18 See Sallam (2018).

19 See Munusamy (2018); Gurumurthy and Vasudevan (2018); Anasuya (2018).

20 See Kee and Randhawa (2010).

21 See GenderIT (2015).

22 See Tucker (2020).

23 See 7amleh Arab Center for Social Media Advancement (2018).

24 See Fascendini (2014).

25 See GenderIT (2018a).

Feminist Principles of the Internet

In 2014, APC organized a Global Meeting on Gender Sexuality and the Internet in Malaysia to discuss the rights of women, gender-diverse people and LGBTQ+ people on the internet. Fifty participants from six continents gathered to collaborate on how to merge gender and sexual human rights with the internet rights movement. They developed 15 feminist principles of the internet.[26] These principles outlined a feminist perspective on internet access, resistance movements, transformative spaces, TFGBV, amplifying women's voices, inclusion of more feminist and LGBTQ+ people in decision making, alternative forms of economic power, open-source technologies, access to information, protecting privacy, accessing personal data, resisting the regulation of consensual sexual activity, ensuring a safe internet for children, problematizing the concept of pornography as inherently harmful and protecting anonymity. An updated version of the Feminist Principles of the Internet was released in 2016.[27] This document focused on access to technology and information; social movements and public participation online; encouraging alternative economies; amplifying and protecting feminist expression; and building agency for women, LGBTQ+ and gender-diverse people online, including by addressing TFGBV.

Feminist Internet Research Network

The Feminist Internet Research Network is a group of global researchers "build[ing] an emerging field of internet research with a feminist approach, to inform and influence activism and policy making."[28] The main issues this research network addresses are datafication, OGBV, digital access, and economy and labour. Through this research network, APC works in collaboration with various other feminist and digital rights organizations to produce publications. Some of their most recent reports include *Power X Expression X Violence: A Research on Women's Freedom of Expression on Social Media in Malaysia* (KRYSS Network); *After the Storm: How to Restore Policy Dialogue and Supportive Discourse against*

26 See https://genderit.org/articles/feminist-principles-internet.

27 See www.apc.org/en/pubs/feminist-principles-internet-version-20.

28 See www.apc.org/en/pubs/feminist-internet-research-network-meta-research-project-report.

Gender-Based Violence Online in Bulgaria (BlueLink Foundation); *Anti-rights Discourse in Brazilian Social Media: Digital Networks, Violence and Sex Politics* (Latin American Center on Sexuality and Human Rights); and *Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet* (Pollicy).

Derechos Digitales

Derechos Digitales is a Latin American digital rights organization that was founded in 2005.[29] It promotes human rights in the digital sphere, specifically focusing on freedom of expression, privacy and data collection, and copyright and access to information. It provides legal and technical research, education and policy advocacy on digital rights. Derechos Digitales approaches gender as a cross-cutting theme in its work. Its team is gender balanced and they have policies in place to secure diversity and gender approach in their research and staff work.

Derechos Digitales is very concerned with the reproduction of offline exclusions and inequalities in the digital world and has been working to advance opportunities for historically marginalized groups to enjoy their rights online. In 2017, Derechos Digitales produced their landmark report *Latin America in a Glimpse*, which focused on mapping and providing visibility to gender information and communication technology initiatives in the region.[30] This work helped the organization communicate the challenges that women who actively participate in the internet ecosystem in Latin America confront daily as a continuum of the violence they suffer in the physical space in their activism.

In recent years, Derechos Digitales has developed and supported campaigns and trainings specifically directed to women's security online, looking at the gender-differential impact on threats and risks confronted on the internet. By working with women collectives based in Bolivia, Chile, Colombia, Ecuador, Guatemala and Mexico, the organization has developed methodologies for conducting assessment and training in digital security from a feminist perspective.[31] It has also concentrated efforts in supporting local organizations in responding to gender gaps and online gender violence in the region through its Rapid Response Fund for the Protection of Digital Rights in Latin America.[32]

Derechos Digitales's work has been focused on demonstrating the ways that the data, algorithms and protocols that the internet is built over are not neutral in terms of gender. It has published about the gendered impacts of the deployment of identity systems in Latin America,[33] the impacts on freedom of expression from a gender perspective,[34] crimes against intimacy,[35] anonymity and encryption and TFGBV,[36] and it has proposed a feminist framework for artificial intelligence (AI).[37] Finally, Derechos Digitales has dedicated efforts to making sure Latin American women's voices are considered in the development of internet protocols, working jointly with other organizations to influence the Internet Engineering Task Force for the development of standards that consider human rights and feminist principles.[38]

Internet Democracy Project

The Internet Democracy Project, based in New Delhi, India, was established in 2011.[39] Its work aims to use the Indian context as a starting point, then develops what it has learned to apply to a wider context. It is "working towards realising feminist visions of the digital in society by exploring & addressing power imbalances in the areas of norms, governance & infrastructure."[40] Its work addresses a wide variety of topics related to women, gender, sexuality and the internet, including TFGBV. It has applied a feminist perspective to data collection,[41]

29 See www.derechosdigitales.org/.

30 See Paola et al. (2017).

31 Derechos Digitales has supported and participated in the work of the grassroots organization Ciberseguras. See https://ciberseguras.org/.

32 See Derechos Digitales (2021).

33 See Díaz and Venturini (2020).

34 See Acosta (2020).

35 See Hernández (2020).

36 See Canales (2017).

37 See Silva (2022).

38 See Guerra and Knodel (2019).

39 See https://internetdemocracy.in/.

40 See https://internetdemocracy.in/about-us.

41 See Jain (2021).

sexuality online,[42] surveillance,[43] online harassment and the law,[44] verbal online abuse[45] and other issues connected to gender and the internet. In addition to research, the Internet Democracy Project engages in policy development and has released policy briefs on topics such as feminist principles on consent in data governance[46] and online violence against women.[47] It has also organized multiple meetings and conferences on gender and the internet, along with Point of View, including Porn. Panic. Ban: A Conversation on Sexual Expression, Pornography, Sexual Exploitation, Consent;[48] My Troll, Our Troll? Moving beyond Individual Action and towards Structural Change against Online Abuse;[49] and Imagine a Feminist Internet South Asia.[50] These conferences bring people together to discuss issues such as women's sexuality, sexual expression, privacy and TFGBV.

Chenai Chair (Various Organizations)

Chenai Chair has worked at the intersection of digital technology and gender, assessing the impact of technology on society. Her work draws on principles of feminism to assess digital technology. Chenai was a Mozilla 2019/2020 Tech Policy fellow.[51] She developed a feminist project focused on privacy, data protection and AI known as "My Data Rights (Africa)."[52] Her research includes a project that examined the ways that African feminists in Malawi, South Africa, Zambia and Zimbabwe engage on issues to do with gender, privacy and data, including resisting digital rights violations.[53] Chenai has further developed a research project aimed at understanding the Southern African Development Community's model laws framing of gender and sex life and African feminist resistance to extractive data practices. Her work is available on mydatarights.africa.

Chenai led the development of research and writing of the 2020 report *Women's Rights Online: Closing the digital gender gap for a more equal world* for the World Wide Web Foundation.[54] This report provided a global snapshot of the state of digital gender inequality, focusing on Colombia, Ghana, Uganda and Indonesia. It found that even where women are closing the gap on basic internet access, they face a multitude of additional barriers to using the internet and fully participating online.

Chenai also developed research projects that sought to provide evidence to bridge the digital divide and to understand the experiences of young people accessing the internet in Africa while at Research ICT Africa.[55] She has worked in collaboration with Pollicy on Afrofeminist Data Futures, a project that "seeks to better understand how feminist movements in sub-Saharan Africa can be empowered through the production, sharing and use of gender data, and how this knowledge can be translated into actionable recommendations for private technology companies in terms of how they share non-commercial datasets."[56] She has also worked on a project, Engine Room, that seeks to understand the lived experiences of people using digital ID systems in mostly marginalized communities in Bangladesh, Ethiopia, Nigeria, Zimbabwe and Thailand.[57] Chenai is currently a senior program officer at the Mozilla Foundation leading the development of Mozilla's Africa Innovation Mradi and Common Voice programmatic work.[58]

42 See Bhandari and Kovacs (2021); https://internetdemocracy.in/events/imagine-a-feminist-internet-research-policy-and-practice-in-south-asia.

43 See Radhakrishnan (2020).

44 See Padte and Kovacs (2013).

45 See Kovacs, Padte and Shobha (2013).

46 See Kovacs and Jain (2021).

47 See Chandrasekar (2017).

48 See https://internetdemocracy.in/events/porn-panic-ban.

49 See https://internetdemocracy.in/events/my-troll-our-troll.

50 See https://internetdemocracy.in/events/imagine-a-feminist-internet-research-policy-and-practice-in-south-asia.

51 See https://foundation.mozilla.org/en/blog/authors/chenai-chair-33/.

52 See https://mydatarights.africa/.

53 See https://mydatarights.africa/projects/.

54 See https://webfoundation.org/research/womens-rights-online-2020/.

55 See https://researchictafrica.net/author/chenai-chair/.

56 See https://pollicy.org/projects/afro-feminist-data-futures/.

57 See https://digitalid.theengineroom.org/assets/pdfs/200123_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive.pdf.

58 See https://foundation.mozilla.org/en/blog/going-far-together-mozillas-africa-innovation-mradi-focus/.

International Development Research Centre

The International Development Research Centre (IDRC) was established by an act of Canada's Parliament in 1970, and functions as part of Canada's international aid envelope.[59] IDRC champions and funds research and innovation within and alongside partners in the Global South to drive global change — investing in high-quality research, sharing knowledge with researchers and policy makers for greater uptake and use, and mobilizing global alliances to build a more sustainable and inclusive world.

IDRC has supported research on the governance of technologies for much of its 50-year history. In the past decade, the centre has invested critical research monies to support a more feminist, equitable internet[60] to help stakeholders and policy makers understand the new reality of the online and digitally driven world. Investments include foundational research on the gendered digital divide,[61] countering sexist hate speech,[62] building the field of feminist internet research,[63] supporting feminist AI,[64] shaping the global research agenda on feminist data governance[65] and understanding the landscape of cybersecurity for LGBTQ+ communities,[66] as well as this first statistically meaningful survey in the Global South on OGBV.[67] IDRC is also aligning with Canada's efforts in the Freedom Online Coalition[68] to expand the engagement of Global South experts in shaping norms and national legislation to address misinformation and TFGBV. The aim is to enable development, private sector and government stakeholders to use this research and data to improve their responses to TFV and hate speech. Another objective is to ensure that scholars, advocates and researchers in the Global South — equipped with their findings and policy ideas — have a voice at the table when laws and regulatory measures are discussed. The hope is that this rich body of research from Global South experts will have a substantive and long-term impact in national and international policy spaces on the equitable and fair governance of the digital public sphere.

59 See www.idrc.ca/en/about-idrc.

60 See https://firn.genderit.org/.

61 See www.idrc.ca/en/project/understanding-digital-access-and-use-global-south.

62 See www.idrc.ca/en/project/recognize-resist-remedy-research-project-combat-gender-based-hate-speech-against-women.

63 See www.idrc.ca/en/project/making-feminist-internet-research-network.

64 See www.idrc.ca/en/project/advancing-research-feminist-artificial-intelligence-advance-gender-equality-and-inclusion.

65 See www.idrc.ca/en/project/data-inclusive-democratic-and-feminist-development-shaping-global-research-agenda.

66 See https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/.

67 See www.idrc.ca/en/project/supporting-safer-internet-2-global-survey-tech-facilitated-gender-based-violence.

68 See https://freedomonlinecoalition.com.

Introduction

Digital spaces, such as social media platforms and instant messaging via text or apps, can be incredibly uplifting places where women and LGBTQ+ people go to find information, build community and gather support. These tools are used to create and maintain valuable allies, friendships and other caring relationships.

They are essential for democratic discussion, advocacy, creativity and education. They have been used by these communities in creative ways to build movements and create resistance against the discriminatory status quo. These digital spaces must be protected and nurtured so that all people can benefit from them.

Unfortunately, the current digital landscape is one where the cruellest voices often dominate and discriminatory hierarchies are reinforced through negative engagement in digital spaces, preventing women and LGBTQ+[69] people from participating freely, safely and authentically in them. The data discussed in this report affirms that this unhealthy digital environment exists, and that women and LGBTQ+ people suffer disproportionately. The data shows that people are often specifically targeted because they are members of equity-seeking groups, that there is a lack of effective resources and supports available for all people being harmed online, and that far too many people are suffering in silence. A digital world in which people are discriminatorily targeted because of their gender, sexual orientation and other intersecting aspects of their identity without meaningful redress can never fulfill the true potential of digital spaces that is afforded with equitable inclusion.

This report will provide background information on technology-facilitated gender-based violence (TFGBV) and technology-facilitated violence (TFV) against LGBTQ+ people by summarizing some of the existing research on this topic. It will then present quantitative data collected on people's experiences with, and opinions of, 13 forms of online harm that have been recognized as common forms of TFGBV and TFV against LGBTQ+ people. The survey discussed in this report specifically examines people's online experiences. Many forms of TFGBV involve modern digital technologies that are not connected to the internet, such as cellphones that are not internet connected, GPS location tracking devices or cameras that are not connected to the internet to perpetrate voyeurism. However, the data collected for this report focuses solely on online experiences and will therefore use the terms online harms and online gender-based violence (OGBV) when discussing the data collected as it focuses specifically on online experiences. OGBV is a subset of the larger issue of TFGBV.

Although the analysis of this data is focused on the experiences of women and LGBTQ+ people, this survey collected data from people of all genders and sexual orientations. Data was collected from cis and trans women and men, gender non-conforming, agender, non-binary people and people of other gender identities, as well as gay, lesbian, bisexual, heterosexual and other sexual orientations.

This report includes data on the type of online harms participants experienced, how harmful they thought these forms of online harm were, how they were impacted by their experiences with being harmed online, how people responded to online harms, and what resources and supports they used and thought might help people targeted by OGBV. The data is used to examine the influence of gender identity, gender expression and sexual orientation, in particular, on these types of online harm.

The report is divided into three main sections. The first section focuses on the experiences and impacts of online harms on victims/survivors. The second section focuses on the resources and supports that victims/survivors have used and would like to see. These two sections begin with background information on TFGBV, followed by detailed descriptions of the survey results, and conclude with summaries on how gender and sexuality are reflected in the data to expose what represents OGBV and online violence against LGBTQ+ people. The final section includes a list of recommendations for governments, technology companies, academics, researchers and civil society organizations on how they can contribute to addressing and ending TFV.

This report aims to centre on the experiences of people from the Global South and includes data from many countries in the Global South. The authors would like to recognize that the term "Global South" is a contested term, and that this terminology is not the sole nor universally

69 LGBTQ+ (lesbian, gay, bisexual, transgender, queer or questioning and other non-heterosexual sexual orientations, and gender-diverse identities) is the standard abbreviation used to describe the LGBTQ+ community in CIGI publications. However, we recognize that there are a variety of abbreviations used, such as LGBTQIA2S+, LGBTQQIP2SAA, 2SLGBTQ+ and others, that represent a range of gender identities, gender expressions and sexual orientations. The authors' analysis is meant to be inclusive of that wide diversity.

The current digital landscape is one where the cruellest voices often dominate and discriminatory hierarchies are reinforced through negative engagement in digital spaces, preventing women and LGBTQ+ people from participating freely, safely and authentically in them.

accepted term used to describe regions of the world that include countries that are systematically lesseconomically and politically advantaged. Some prefer to call these regions the "majority world," in the Global South, it was decided to use the term Global South, while recognizing the term's limitations.

Data was collected from 18,149 people of all genders in 18 countries (Algeria, Argentina, Brazil, Canada, Chile, China, Colombia, Ecuador, France, Germany, India, Jordan, Kenya, Saudi Arabia, South Africa, Tunisia, the United Arab Emirates [UAE] and the United States). Participants in Algeria, Jordan, Saudi Arabia, Tunisia and the UAE were not asked to report their sexual orientation or diverse gender identity due to safety and legal limitations in those countries.

The purpose of this report is to centralize the experiences of women and LGBTQ+ people with TFGBV and TFV against LGBTQ+ people in the Global South. As noted in the earlier section on the project's steering committee, civil society organizations and researchers in the Global South have long been the thought leaders on these issues, having engaged in research, advocacy and education on this issue for decades. The data in this report hopes to supplement and build on that existing research, as well as on research and data from other regions. People in the Global South have unique and culturally specific needs that must be addressed by TFV research, laws and policies, including technology companies' policies. Countries in the Global South often have fewer resources to address TFV, may have challenges with the rule of law and struggle to get technology companies to recognize and act on the contextual, linguistic and cultural needs of people in their regions. As such, it is critical that more attention be brought to the experience of those living in the Global South.

In addition to a focus on countries of the Global South, this report examines the experiences of women and LGBTQ+ people with online harms in particular. Gender-based violence and violence against LGBTQ+ people are rampant in digital spaces. TFV against these groups violates their human rights and negatively impacts their experiences in their overlapping physical and digital worlds. Cis women and girls, transgender people, gender non-conforming, agender and non-binary people, as well as bisexual, lesbian and gay people, are discriminatorily targeted with TFV because of their gender, gender identity, gender expression and sexual orientation, leaving many of them feeling unsafe in digital spaces and in the physical world, with many facing discriminatory violence against them. Their digital and physical experiences are inseparable in the modern world. Negative digital experiences will inevitably impact the physical experiences of those targeted, causing mental distress, impacting their general feelings of safety and, in some cases, leading to physical violence. Conversely, negative experiences in the physical world will be shared and reflected in digital spaces and impact how people engage in these spaces.

Previous research has shown that women and LGBTQ+ people are targeted by abusers online because of their gender and sexual orientation, and that these groups are uniquely vulnerable to the impacts of certain forms of TFV, such as the non-consensual distribution of intimate images (NCDII)

and stalking.[70] For example, some cyberstalking apps are marketed as tools to spy on current and ex-intimate partners and can be used as tools to commit gender-based violence in intimate partner relationships (Parsons et al. 2019), "revenge porn" websites predominantly host sexual images of women shared without their consent (Henry and Flynn 2019), and women and girls more commonly have their devices monitored and controlled by male family members (Udwadia and Grewal 2019). In recent years, hate groups have increasingly targeted LGBTQ+ people both online and off. Misogynistic, transphobic and homophobic groups, and their influential leaders, provoke networked harassment against women and LGBTQ+ people (Yahaya and Iyer 2022; Curlew and Monaghan 2019), along with anyone who does not fit within sexist, homophobic and transphobic discriminatory norms or those who dare to advocate for gender equality or LGBTQ+ rights (Posetti 2017; Palumbo and Sienra 2017). These are just a few ways that technology is used to harm women and LGBTQ+ people in digital spaces. It is critical to recognize that gender and sexuality are not the only identity factors that make women and LGBTQ+ people vulnerable online. Women and LGBTQ+ people who are Black or Indigenous, are people of colour, have disabilities or are discriminated against because of their ethnicity or religion face compounding harms related to their intersecting social locations (United Nations Human Rights Council 2018). The experiences of women and LGBTQ+ people, including those with these intersecting identities, will be reflected in the findings from this survey, wherever possible.

70 See, for example, Kovacs, Padte and SV (2013); Vogels (2021); Human Rights Watch (2020); Powell and Henry (2015).

Misogynistic, transphobic and homophobic groups, and their influential leaders, provoke networked harassment against women and LGBTQ+ people.

Key Findings in Brief

The results of the survey will not be surprising to anyone who has spent time online. Research shows that TFV and online harms are widespread. The data demonstrates the disproportionate negative impact of online harms on women and LGBTQ+ people:

- Almost 60 percent (59.7 percent) of all participants had experienced at least one of the 13 forms of online harm surveyed.
- Transgender and gender-diverse people reported the highest proportion of incidents experienced, with cis women reporting slightly higher proportions of incidents of online harm compared to cis men.
- Although men and women reported relatively similar numbers of incidents of online harm in several categories, women were much more likely to report a serious impact from online harms compared to men.
- LGBTQ+ people were much more likely to report a serious impact from online harms compared to heterosexual people.
- Women were much more likely to rate the various forms of online harm as harmful compared to men.

Women reported similar or higher proportions of incidents of online harm in many categories compared to men; however, when asked what their general opinions were on various forms of online harm, women consistently rated almost all forms of online harm as more harmful than men, which reflects much of the research showing that women are more negatively impacted by online harms than men. Surprisingly, transgender and gender-diverse people generally rated most forms of online harm as less harmful than men and women, even though as individuals they reported proportionately more incidents of harm and more serious impacts than most other groups. This may be due to a normalizing effect, where some people who experience TFV more regularly and do not find support from society about the harms that they experience may start to downplay its overall effects because the experience is so common and is regularly dismissed by the general public. The data indicated similar results in young people, who, like transgender and gender-diverse people, experienced a higher prevalence and more negative impacts of online harms, but also rated many categories of online harms as less harmful generally. The harms faced by transgender, gender-diverse and young people may be downplayed by society in ways that impact their overall conceptions of these harms. This potential normalization of TFV among those groups that are most impacted is a disturbing trend.

Survey participants were aware of the disproportionate challenges that women and LGBTQ+ people face in digital spaces. A significantly higher proportion of participants recognized that OGBV was a serious issue for women and LGBTQ+ people compared to men. When participants were asked who OGBV was a big problem for:

- 46.5 percent reported that it was a very big problem for LGBTQ+ people;
- 44.3 percent reported that it was a very big problem for women; and
- 22.7 percent reported that it was a very big problem for men.

Gender differences were also apparent in who perpetrated the various forms of online harm. The data shows that men's behaviour in digital spaces contributes to much of the most harmful forms, including OGBV and online violence against LGBTQ+ people. A high proportion of participants reported that men were the perpetrators of the most serious incidents of TFV they experienced:

- Close to half of all participants (49.7 percent) reported that a man perpetrated the most serious digital attack they personally experienced; a smaller percentage (18.9 percent) reported that a woman was the perpetrator.
- More than half of women (57.7 percent) and transgender and gender-diverse people (51.6 percent) reported that it was a man who targeted them, compared to 42.9 percent of men.
- Almost one-quarter of participants (24.8 percent) could not identify the gender of the person (for example, when the person used an anonymous user profile that did not indicate their gender).

- A very small percentage (1.1 percent) of participants reported a person of an "other" gender was the perpetrator.[71]

The identity of an individual played an important role in why they were targeted. Of the most serious incidents of online harm experienced, most participants reported that they were targeted because of their gender identity, gender expression, sexual orientation, race, religion or disability:

- Transgender and gender-diverse people (31.8 percent) and women (29.8 percent) were more likely to report they were targeted because of their gender identity than men (16.0 percent); lesbian, gay, bisexual and other sexualities (LGB+) people (27.8 percent) were more likely to be targeted because of their gender identity than heterosexual people (23.0 percent).
- Transgender and gender-diverse people (24.0 percent) were more likely to report they were targeted because of their gender expression than men (8.6 percent) and women (8.2 percent), as were LGB+ people (17.8 percent) compared to heterosexual people (7.8 percent).
- LGB+ people were more likely to report they were targeted (42.7 percent) because of their sexual orientation than heterosexual people (6.6 percent).

Additionally, the data showed that people are struggling to talk to others about experiencing online harms and to find effective support and resources. Very few spoke to anyone about their experience. Of those that did reach out for help, few formal mechanisms were rated as "very effective," showing that there is a long way to go in creating and improving support for victims/survivors of TFV. This issue is particularly relevant in the Global South, where there are often fewer laws related to TFV in place, there may be challenges with the rule of law and there are fewer resources available for victims/survivors of TFV. Among the most serious incidents of online harms:

- Almost 40 percent (39.6 percent) of people did not reach out to anyone for help, not even friends or family.
- Very few (10.1 percent or less) sought support from social media companies, government services, including the police, or civil society organizations.

This data demonstrates that online harms are a rampant and serious issue that needs more attention, and that particular attention needs to be paid to the experiences of women and members of the LGBTQ+ community, who are more significantly impacted by TFGBV.

Almost

% of all participants had experienced at least one of the 13 forms of online harm surveyed.

71 A small percentage of participants (5.5 percent) selected "Prefer not to answer."

Data was collected from

18,149

people of all genders in **18** countries.

Algeria
Argentina
Brazil
Canada
Chile
China
Colombia
Ecuador
France
Germany
India
Jordan
Kenya
Saudi Arabia
South Africa
Tunisia
UAE
United States

Methodology

This report selected a broad range of countries, focusing mainly on countries located in the Global South, to provide diverse representation of people who have experienced online harms internationally and to create data in regions where data collection on online harms is sparse or non-existent. Data was collected from 18,149 people of all genders in 18 countries: Algeria, Argentina, Brazil, Canada, Chile, China, Colombia, Ecuador, France, Germany, India, Jordan, Kenya, Saudi Arabia, South Africa, Tunisia, the UAE and the United States. Approximately 1,000 people per country were surveyed, primarily through online surveys. In countries with lower internet penetration (Algeria, Brazil, Colombia, India, Kenya, South Africa and Tunisia), in-person and telephone interviews were conducted as well as online surveys.

Categorization of Gender and Sexual Orientation

The following section details how gender and sexual orientation were categorized in the analysis of the data for this report.

Gender Data Categorization

When analyzing the data, gender was categorized in these ways: for sex/gender identity, any participant who selected a single gender or sexual identity (male/man or female/woman, that is, cisgender man or woman) that was congruent with their reported sex was categorized as a singular gender (man/woman). As such, when reading statistics from this report that refer to "women" or "men," this categorization should be read as cis women and cis men (although some transgender people may have selected gender-matching categories, depending on how they personally identify). Participants who reported incongruent sex/gender or sexual identity, selected "another gender identity" or provided genders of "diverse" or "other" for sex or gender identity (male and woman, female and man, diverse or another gender identity) were categorized as transgender and gender diverse. Transgender women and men were included in this category, rather than the larger category of cis women and men, as they face unique forms of discrimination that are aligned with those faced by gender non-conforming, agender and non-binary people. As such, statistics that refer to "transgender and gender-diverse people" should be considered as inclusive of transgender, gender non-conforming, agender and non-binary people as well as anyone outside of the cisgender binary.

The authors recognize that a person's gender identity can include identities other than those listed here, such as two-spirit, agender, genderqueer, non-binary or other gender categories. "Gender diverse" is being used as an umbrella term in this report to capture any gender identity outside of the cisgender binary; however, the authors acknowledge that this term may be underinclusive for some and overinclusive for others. No term can accurately capture the complexity of all gender identities.[72]

In addition, the authors would like to acknowledge the challenges that come with categorizing people within discrete gender categories, in particular for larger quantitative data sets of the general population. Gender is a social construct that lies on a continuum and cannot fit perfectly within discrete boxes. However, in a quantitative study, some categories were required for analysis. These categories have limitations. For example, transgender and cisgender women's shared experiences as women, including experiencing harmful forms of TFGBV targeted at women online, such as sexual harassment, suggests that they should be analyzed under a single gender data category. Separating transgender women from the category of "women" (which only represents cis women in this analysis) systemically others transgender women. At the same time, transgender women have experiences of TFV that are unique to them, but which are similar to those experienced

72 Of all participants, 5,565 were not asked to report their gender identity (man, woman, a diverse gender identity, another gender identity or if they identified as cis gender or not) or their sexual orientation due to limitations in the country that made it unsafe to ask (in Algeria, Jordan, Saudi Arabia, Tunisia and the UAE).

by transgender men and gender-diverse people, such as transphobic attacks.

The authors chose to categorize gender this way to highlight the experiences of transgender and gender-diverse people, rather than to systemically exclude transgender people within the larger categories of men and women. This was done because the small number of transgender women, men and gender-diverse people did not allow for a statistically significant analysis of those categories individually. Categorizing gender identity in these ways means that the important data on transgender and gender-diverse people features definitively in the results, allowing for analysis on the specific harms transgender and gender-diverse people face in digital spaces, which were essential to feature.

Sexual Orientation Data Categorization

When analyzing the data, sexual orientation was categorized in the following way: any participant who selected non-heterosexual options (lesbian, gay or another sexual orientation) or multiple sexual orientations (heterosexual and another option, or options beyond heterosexual) were categorized as LGB+ (lesbian, gay, bisexual or other sexual orientation); any participant who only selected heterosexual was categorized as heterosexual. Of those who were asked and reported their sexual orientation, 92 percent identified as heterosexual, and 8.0 percent identified as LGB+.

The authors would like to recognize that there is a wide diversity of ways that people define their sexual orientation, such as queer, pansexual, two-spirit, demisexual and many more. The term "LGB+" was chosen as an umbrella term for this report, however, the authors recognize that this is a simplified term that does not fully capture the breadth of people's diverse sexual orientations.

Analytic Strategy to Examine Intersectionality

Intersectionality of gender and sexuality was examined with multi-way frequency analysis (MFA). This nonparametric analysis is similar to an analysis of variance for categorical variables, which compares observed and expected frequencies (Tabachnick and Fidell 2019). Inadequate expected cell frequencies (i.e., 20 percent of cells under five) (ibid.) can influence the results of MFA. To address this issue, the authors used gender diversity (transgender and gender diverse, women and men) rather than an interaction between biological sex and gender identity. In these analyses, form of online harm (experienced or not) was conceptualized as the dependent variable. Independent variables included gender diversity (transgender and gender diverse, women and men) and sexual orientation (LGB+ and heterosexual), yielding expected cell frequencies that exceeded five in all cases. Traditionally, MFA is used to create a model by testing the higher-order associations (for example, gender diversity by sexual orientation by online harm) followed by all two-way, then one-way associations. Non-statistically significant associations were eliminated from the model. Since the authors were not interested in establishing a model, analyses were restricted to the examination of variations in experiences of online violence as a function of gender diversity and/or sexual orientation (following procedures by Vaillancourt et al. 2021). A statistically significant three-way interaction was considered evidence of intersectionality, and results reported accordingly. Proportions were further examined using chi-square tests of association and differences were assessed using the z-test for column proportions. MFA was also used to examine the effects of intersectionality on the impacts of online harms as well as perceptions of harmfulness. The McNemar's test was used to compare the paired proportions of participants reporting who OGBV was a big problem for. Because the analysis did not control for multiple comparisons (Hsu 1996) using a false discovery rate procedure such as Benjamini-Hochberg (Benjamini and Hochberg 1995), the probability of committing false statistical inferences was increased.

The data set and SPSS syntax used to generate the statistics in this report are available upon reasonable request to the authors. Some data have been suppressed to ensure that participants cannot be identified if data with small sample sizes are combined. The full results of inferential statistics can be found in the Appendix.

Limitations

The following limitations need to be considered when interpreting the findings in this report.

First, convenience samples were used so the findings may not generalize to the population or certain subgroups. Second, the data was collected during the COVID-19 pandemic, a time when TFGBV increased worldwide (Kraicer 2020). Thus, the issues highlighted in this report may be more pronounced than those documented before the pandemic. Third, missing data for some countries is high, which can impact statistical inferences. In particular, the sample sizes for LGB+ and transgender and gender-diverse people were proportionately lower than heterosexual and gender binary people, respectively. Therefore, reported percentages for LGB+ and transgender and gender-diverse groups, as well as cross-tabulations, may have a larger margin of error and be less reliable than those reported for heterosexual people and men and women. Fourth, there may be error induced by the coding of gender in this report as some transgender people may have identified with gender-matching categories. For these reasons, some of the raw percentage differences involving any of these groups may be larger than those not involving these groups, yet not statistically significantly different. Fifth, the data is cross-sectional, which precludes comments about causation. Sixth, it is possible that responses of "Prefer not to answer" and "Don't know/not sure," which were treated as missing in data analyses, were systematically missing. In this report, missing data mechanisms were not examined. Failure to examine and manage underlying patterns of missingness, in conjunction with a per analysis listwise deletion analytic strategy, may lead to bias in estimates.

Gender is a social construct that lies on a continuum and cannot fit perfectly within discrete boxes.

Section I

TFV: Incidents and Impacts

The following section discusses TFV and the broader influence of gender and sexual orientation on the 13 types of online harm participants in the global survey were asked about. It then reviews the number of incidents participants reported, the impact of the online harm and how harmful they found each behaviour to be.

Survey participants were asked whether they had experienced any of these 13 forms of online harm:

1. Physically threatened online (e.g., a death threat, rape threat, threat of physical harm)
2. Blackmailed online (e.g., someone threatening to post private information about them unless they did something in return, including sextortion)
3. Monitored, tracked or spied on online (e.g., by GPS location, or someone keeping track of what they say or do online)
4. Someone accessing devices or social media accounts belonging to them without permission
5. Called discriminatory names or derogatory cultural terms (e.g., sexist or racist names)
6. Personal nude or sexual images of them shared or shown to someone else or posted online without permission (non-consensual use of intimate images)
7. Unwanted sexual images sent to them
8. Having personal contact information or address posted online without permission (doxing)
9. Lies posted online about them (defamation)
10. Online impersonation (e.g., someone makes a fake account of them)
11. Repeatedly contacted by someone they do not want to be contacted by
12. Networked harassment (e.g., a group of people organized online attacks against them)
13. Experienced harassment online because of their gender, race, sexual orientation, disability, gender expression or other marginalizing factors (gendered harassment)

As the focus of this research was to look at the influence of gender and sexual orientation on these online harms, these specific forms of harm were selected as they are commonly identified as forms of TFGBV and TFV experienced by LGBTQ+ people in previous research (Iyer, Nyamwire and Nabulega 2020; Amnesty International 2018; Goulds et al. 2020; GenderIT 2018b; Van Der Wilk 2018).[73]

73 See also https://onlineviolencewomen.eiu.com/.

Introduction: TFV

In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Jane Bailey, Nicola Henry and Asher Flynn define technology-facilitated violence and abuse as "an umbrella term used to describe the use of digital technologies to perpetrate interpersonal harassment, abuse, and violence" (Bailey, Henry and Flynn 2021, 1).

It includes technology-facilitated behaviour such as hate speech, trolling, image-based sexual abuse, threats, doxing and stalking. TFV can happen to anyone, regardless of their gender, sexual orientation or other social locations (Dunn 2020a). It can be used to cause generalized harm to individuals but can also cause specific systemic discriminatory harms against equity-seeking groups and individuals, such as women and LGBTQ+ people.

For example, organizations such as Pollicy, Musawah, the Internet Democracy Project and APC describe how certain conservative political, community and religious leaders in the Global South reinforce patriarchal and heteronormative notions online by disparaging and threatening people they do not approve of, such as feminists, members of the LGBTQ+ community or racial, religious and ethnic minorities (Yahaya and Iyer 2022; Kovacs, Padte and SV 2013; Palumbo and Sienra 2017). This can lead to additional TFV by other community members who are influenced and emboldened by their leaders' actions to further harass the people or groups online, thus reinforcing the discrimination on a grander scale. The spread of negative ideas about women and LGBTQ+ people and their communities legitimizes technology-facilitated and physical violence against them. Similarly, in the Global North, there has been an increase in alt-right groups that endorse racist, misogynistic, anti-feminist, transphobic, homophobic, Islamophobic and anti-Semitic views (McGinley 2022; Sugiura 2021; Conway, Scrivens and Macnair 2019). When a specific woman or LGBTQ+ person is named by an influential member or group of the alt-right, it can lead to sustained harms against that person, including TFV that causes risks to their safety (Curlew and Monaghan 2019; Brown, Sanderson, Silva Ortega, 2022). These discriminatory beliefs are fuelled in online spaces and have been linked to mass murders motivated by racism, homophobia and misogyny (McGinley 2022; Baele, Brace and Coan 2019; Silva and Greene-Colozzi 2019).

The spread of negative ideas about women and LGBTQ+ people and their communities legitimizes technology-facilitated and physical violence against them.

International human rights organizations, such as the United Nations, recognize that certain groups of people experience systemic discrimination in societies at large that violates their human rights, and that these discriminatory practices have moved into digital spaces, including gender-based violence (UN Women 2023b; United Nations Human Rights Council 2018; Coombs 2021). Various experts and bodies within the United Nations have recognized that people can be discriminated against based on gender (UN Committee on the Elimination of Discrimination against Women 2017; United Nations General Assembly 2018), sexual orientation (United Nations General Assembly 2018), race or ethnicity,[74] religion,[75] age,[76] disability[77] and other equality-based identity factors. TFV can be used as a tool to reinforce any of these existing discriminatory power structures, which legitimize sexism, homophobia, transphobia, racism, colonialism, casteism, religious discrimination and others. This discrimination leads to inequality and violence against these groups.

What this means is that when TFV is used as a tool of oppression against equity-seeking groups,

74 *International Convention on the Elimination of All Forms of Racial Discrimination*, 7 March 1966, 660 UNTS 195 (entered into force 4 January 1969).

75 *United Nations Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief*, GA Res 36/55, 36th Sess, UN Doc A/RES/36/55 (1981).

76 *Convention on the Rights of the Child*, 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).

77 *Convention on the Rights of Persons with Disabilities*, 13 December 2006, 2515 UNTS 3 (entered into force 3 May 2008).

it has a larger systemic impact compared to other forms of TFV. It is used to maintain discriminatory social hierarchies and cause real harms, including individual and systemic violence, to these groups. No form of TFV should be minimized, as all forms of TFV can cause real harms to the people targeted; however, this report seeks to highlight some of the ways that TFV is used as an oppressive tool against groups facing systemic discrimination, with a particular focus on women and LGBTQ+ people.

Various bodies and rapporteurs at the United Nations have acknowledged that women and LGBTQ+ people face discrimination because of their gender identity, gender expression and sexual orientation and are at a heightened risk of violence because of this. For example, in the case of women, the UN Declaration on the Elimination of Violence Against Women (article 1) defines violence against women as any act "that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life."[78] Recently, this has been recognized to include gender-based violence in digital spaces (UN Women 2023b).

In 2018, the United Nations released the report of Dubravka Šimonović, 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 Human Rights Council 2018). It noted that "groups of women, such as women human rights defenders, women in politics, including parliamentarians, journalists, bloggers, young women, women belonging to ethnic minorities and [I]ndigenous women, lesbian, bisexual, and transgender women, women with disabilities and women from marginalized groups are particularly targeted by [TFGBV]" (ibid., para. 28). Soon after this report was released, the world was faced with the COVID-19 pandemic, which moved much of the world online and TFGBV became more widespread (Kraicer 2020). In 2023, the Commission on the Status of Women expressed its deep concern about "the magnitude of various forms of violence, including gender-based violence that occurs through or is amplified by technology and the significant physical, sexual, psychological, social, political and economic harm it causes to women and girls, throughout their life course, infringing on their rights and freedoms, in particular for those in public life" (UN Women 2023b, para. 53).

When TFV is used as a tool of oppression against equity-seeking groups,it has a larger systemic impact compared to other forms of TFV.

It is important to recognize that gender-based violence goes beyond violence directed at cis women and girls (Dunn 2020a). As noted by the Women's Legal Education and Action Fund (LEAF), TFGBV is also aimed at transgender, gender-nonconforming, agender and gender-diverse people because of their gender identity and expression (Khoo 2021). TFGBV includes forms of violence involving the use of digital technology that are aimed at people because of their gender, gender identity or expression. It also includes types of TFV that are disproportionately targeted at gender-marginalized people, such as sexual violence, or cause them disproportionate harm, such as NCDII (Powell and Henry 2017).

Additionally, members of the LGBTQ+ community are especially at risk of TFV due to discrimination against them. In 2018, the United Nations adopted the report of the Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity, Victor Madrigal-Borloz, which recognized violence and discrimination "on the basis of sexual orientation and gender identity and, in particular, their intensity and scope. Gender identity refers to each person's deeply felt internal and individual experience of gender, which may or may not correspond with the sex assigned at birth, including the personal sense of the body (which may involve, if freely chosen, modification of bodily appearance or function by medical, surgical or other means) and other gender expressions, including dress, speech and mannerisms" (United Nations General

78 *Declaration on the Elimination of Violence against Women*, GA Res 48/104, UNGAOR, 48th Sess, UN Doc A/RES/48/104 (1993) at 2.

Assembly 2018). Transphobic and homophobic ideas that purport that there are strictly limited gender and sexual roles, including heteronormative roles, are used to condone violence against those who do not fit within these discriminatory norms (Aghtaie et al. 2018; Ashley 2018a; Ontario Human Rights Commission 2014). These views can be used to normalize and legitimize violence against LGBTQ+ people (Namaste 1996). As such, LGBTQ+ people face high rates of TFV and violence in the physical world (James et al. 2016; Brandwatch 2019). These discriminatory views have found their way onto digital spaces, where LGBTQ+ people are regularly targeted by online attackers.

It is critical to acknowledge that gender and sexual orientation are only two aspects of why someone may be targeted by TFV. The reasons why women and LGBTQ+ people experience violence and discrimination often intersect with additional identity factors. Intersectionality scholarship by Kimberlé Crenshaw (1991) and Patricia Hill Collins (1990) note that a person's gender cannot be separated from other aspects of their identity such as their race, ability, religion, Indigeneity and sexual orientation. For example, women from racial or ethnic minorities experience discrimination (Anwer 2022) in ways that are different from women from the dominant ethnic or racial group (Amnesty International 2018). These intersecting social locations play an important role in how and why people are targeted by TFV.

Finally, as a new phenomenon, there are ongoing discussions about what term should be used when discussing gender and sexuality-based harms that are facilitated by technologies and how to define this form of violence (Wilton Park 2022). Technology-facilitated gender-based violence, or TFGBV, is the most encompassing term for the wider forms of this violence in relation to gender, as it includes non-internet-based violence such as stalking via GPS (Bailey and Dunn, forthcoming 2023). This term has been adopted by international human rights organizations including the United Nations Population Fund (2021). However, there are many subsets of TFGBV, such as OGBV (UN Women 2022), which occur exclusively through internet-connected devices and online spaces, or image-based sexual abuse, which involves the use of sexual images to abuse people (McGlynn and Rackley 2017). When discussing the wider phenomenon, this report will use the terms TFGBV or TFV against LGBTQ+ people but will use the terms online harms and OGBV or online violence against LGBTQ+ people when analyzing the results from the survey as the data specifically examines online experiences.

Transphobic and homophobic ideas that purport that there are strictly limited gender and sexual roles...are used to condone violence against those who do not fit within these discriminatory norms.

Background: Gendered Digital Divide

Before discussing the various forms of TFGBV addressed in this report, it is important to recognize how the gendered digital divide contributes to gender inequality in digital spaces, including TFV. The gendered digital divide is most pronounced in the Global South. According to the Office of the United Nations High Commissioner for Human Rights (2021), women and girls make up the majority of the 3.7 billion people who remain unconnected to the internet worldwide, which reflects the state of gender discrimination globally. The International Telecommunication Union (ITU) reported that in 2020, only 19 percent of women in the least developed countries had used the internet compared to 86 percent in the Global North (in 2019), and, in 2022, 57 percent of women used the internet globally compared to 62 percent of men.[79] The ITU identifies four main categories of the global digital gender divide:

- a gap in access and use of the internet;
- a gap in digital skills and use of digital tools;
- a gap in participation in science, technology, engineering and math (STEM) fields; and
- a gap in tech sector leadership and entrepreneurship.[80]

The digital divide can lead to the silencing of women and can negatively impact their human rights.

This divide limits not only the number of women and girls who can access digital spaces, but also the freedom they have to engage in those spaces. The digital divide can lead to the silencing of women and can negatively impact their human rights. Additionally, women are excluded from the economic and social benefits afforded from digital technologies and experience increasing rates of TFGBV that are inadequately addressed by states and technology companies, which may result in women self-censoring online due to safety concerns (Arimatsu 2019).

Substantive equal access to the internet and digital devices is essential to achieve gender equality and to give more women and girls power in the technological world. As stated by the World Wide Web Foundation, "Women's equal access to new technologies and their meaningful participation on and through the web is a critical component of women's rights and equality in a digital world. Access to the internet can support women to have a voice in spaces where this was previously denied, challenge gender norms, use information, participate in political and associational networks, and increase their economic independence" (Sambuli, Brandusescu and Brudvig 2018).

Mobile Ownership and Internet Access Gap

A 2022 report by GSMA showed that there was a 16 percent gender gap in the use of mobile phones in the Global South in 2021, with the widest gap in South Asia and Sub-Saharan Africa (Shanahan 2022). A 2018 report by Giorgia Barboni et al. found that in India, 67 percent of men own mobile phones compared to 33 percent of Indian women. The ITU (2022) notes that the gender divide for internet use is also wider in several African and Arab countries. A report by the Collaboration on International ICT Policy for East and Southern Africa found that women in Africa are less likely to have access to the internet and have lower social media use (Kapiyo 2022). This divide reduces women's activity in digital spaces and limits their access to education, independence and safety. The GSMA and Cherie Blair Foundation for Women reported that 93 percent of the women they surveyed from low- and middle-income countries felt safer, 85 percent felt more independent, and 41 percent had increased access to income and professional opportunities, contributing to gender equality, when they have access to mobile phones (GSMA and Cherie Blair Foundation for Women 2013).

79 See www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx.

80 Ibid.

According to the EQUALS Research Group, the digital gender gap is in part due to the high cost of access to technology, women's limited access to economic resources, a lack of digital skills, safety risks and socio-cultural barriers that hinder women's participation (Sey and Hafkin 2019). This divide is further amplified for rural women in the Global South (African Declaration 2015; Sanya 2013) — this rural/urban digital divide remains true for rural and Indigenous communities in the Global North, including in Canada (McMahon, Lahache and Whiteduck 2015; Bailey and Shayan 2016). Interestingly, Alison Gillwald (2018) noted that in some Global South countries, such as India and Bangladesh, the digital gender divide for mobile phone access was more pronounced compared to countries such as Ghana and Kenya, which have similar gross national income per capita, suggesting that affordability and the wealth of a country is not the primary factor in explaining the gendered digital divide. Other gendered aspects may be at play and these cultural factors can negatively influence women's and girls' access to digital tools and spaces.

Patriarchal Control and Access to Devices and the Internet

Women in the Global South often have less access than men to devices such as mobile phones and to the internet, since the men in the family are likely to be given priority in accessing these things (Villamil 2022). However, physical access to a device is not the only gendered limitation. Several authors have noted that when women do have access to devices or the internet, it is common for their use to be monitored by male family members, limiting their freedom of use (Badran 2019; Jamil 2021; Philip 2018). In addition, public spaces for accessing the internet, such as internet cafés, are male dominated in certain countries and can be less welcoming to women, further limiting women's access to these technologies (ibid.). Digital surveillance of women can include the direct surveillance of their devices, as well as indirect monitoring of their public posts and activity on the internet (Odeh 2018). Surveillance of women by male family members and the community limits their ability to express themselves freely and communicate with whom they want. This is further amplified by the gendered critiques of women for having too many friends on social media, interacting with men online, and for posting photos male family members do not approve of, as well as the disproportionate criticism for women who have public-facing social media profiles (Tyers-Chowdhury and Binder 2021).

Surveillance of women by male family members and the community limits their ability to express themselves freely and communicate with whom they want.

Exclusion from STEM Education and Employment in the Technology Sector

A gendered divide is also seen in education and the technology industry. A policy brief by Women 20, a Group of Twenty (G20) engagement group, noted that even among G20 countries, where women and girls are more likely to have access to education, there are fewer women and girls being educated and employed in the information technology sector (Kuroda et al. 2019). Women lag behind in access to employment in that industry (Hupfer et al. 2021). As noted by the World Wide Web Foundation, women, girls and gendered bodies are significantly under-represented in the development of technology, governance and policy making (Sambuli, Brandusescu and Brudvig 2018). Further, gender discrimination and sexual harassment of women in the tech industry can limit their participation by making them unwelcome and unsafe in some of these spaces (Sey and Hafkin 2019). This lack of access, skills, safety and leadership positions for women in the digital sector contributes to broader gender inequality in the tech sector but is also reflected in inequality in digital spaces specifically (Chair, Brudvig and Cameron 2020). The gendered digital divide can lead to a lack of trust in the technology industry's ability and willingness to address women's safety. For example, a study by the World Wide Web Foundation on women's

experiences using the internet in Colombia, Ghana, Uganda and Indonesia found that women were more concerned about their privacy online than men and that they have less trust in online companies to protect their privacy (ibid.).[81]

Lack of Attention to TFGBV and TFV against LGBTQ+ People in Technology Policies

Inequality based on gender and sexual orientation can be seen in technology companies' policies and practices.[82] Although some technology companies have made efforts in recent years to improve their policies, many social media companies have failed to adequately develop or resource their responses to TFGBV (Khoo 2021). Report after report demonstrates that platforms such as Google,[83] Twitter,[84] Instagram[85] and Meta (previously Facebook)[86] are not doing enough to address TFGBV. In her book *The Fight for Privacy*, Danielle Keats Citron (2022) notes that several technology companies have made some efforts to improve their terms of service and content moderation practices to better address TFGBV, in part due to pressure from victim and digital rights advocates, researchers and organizations. However, not enough has been done. Citron points out the many ways that technology companies are not prioritizing the safety and privacy needs of their users. For example, large numbers of victims/survivors of TFGBV and TFV against LGBTQ+ people continue to report that these companies' content moderation processes are lacking and are not responsive enough to fully address their needs and that TFGBV remains common on many platforms (Athar 2015; Khoo 2021). Further, many social media companies prioritize profit, user engagement and data collection over the rights and needs of their users (Zuboff 2019).

A report by the World Wide Web Foundation (2022a) found that social media companies Meta, Google, TikTok and Twitter have made public commitments to address TFGBV; however, addressing TFGBV does not seem to be a primary business priority for these companies, and there is a lack of representation of voices from the Global South in their decision-making processes. For example, APC has noted the lack of commitment from social media companies to adequately address TFGBV in Africa (Iyer, Nyamwire and Nabulega 2020). More culturally specific attention and resources need to be put into social media companies' content moderation practices that aim to prevent and respond to TFGBV.

To properly address gender and sexual orientation discrimination in digital spaces, the gendered digital divide must be eliminated: women and girls need equal access to technology, there needs to be better gender representation within technology companies, the technology industry needs to meaningfully engage with gender and sexuality-equality issues, and specialists and technology companies must improve their responses to TFGBV.

To properly address gender and sexual orientation discrimination in digital spaces, the gendered digital divide must be eliminated.

81 See also https://womenwhotech.org/data-and-resources/state-women-tech-and-startups.

82 See, for example, Horwitz (2021); Wells, Horwitz and Seetharaman (2021).

83 See Amnesty International (2022).

84 See Amnesty International (2018).

85 See Center for Countering Digital Hate (2022).

86 See Horwitz (2021).

Background: Forms of TFV

Although the primary purpose of conducting this survey was to use the data to examine TFGBV and TFV directed at LGBTQ+ people, it should be noted that the 13 types of online harms listed in the survey are not always forms of TFGBV or TFV directed at LGBTQ+ people.

The data from this report includes the experiences of all genders of people, including cis and trans men and women, and gender non-conforming, agender and non-binary people. Not all of their experiences will be forms of these types of gender- and sexual orientation-based harms. For example, if a heterosexual cis presenting man threatens another straight cis presenting man on a social media platform, this is not an example of TFGBV or TFV against LGBTQ+ people. The incident numbers in this report include all experiences with online harms and should be read with this in mind. For example, when asked about the most serious incident of online harm they experienced, male victims were most likely to report being targeted by another man and only a small percentage of participants identified as LGBTQ+. As such, most incidents of online harm reported by men are not TFGBV/OGBV or TFV/online violence against LGBTQ+ people. When examining the number of incidents reported, this should be considered as the numbers represent more generalized experiences with online harms rather than TFGBV and TFV against LGBTQ+ people specifically.

Research on gender-based violence and violence based on sexual orientation looks at groups that are systemically marginalized because of their gender expression, gender identity or sexual orientation, such as women and LGBTQ+ people. In the following section, the influence of gender and sexual orientation on the 13 forms of online harm are discussed by examining previous research on these subjects to show the ways it contributes to the discrimination of women and LGBTQ+ people and to violence against them. Although the survey collected data on online harms experienced and perpetrated by all genders of people, this report is primarily interested in looking at individual and systemic harms impacting equity-seeking communities, particularly those discriminated against because of gender and sexual orientation, and will analyze the data with this focus.

Physical Threats

When threatened in digital spaces, women and LGBTQ+ people are more likely to receive threats of sexual violence, such as rape threats, than heterosexual men (Powell and Henry 2017). This is due, in part, to the gendered and sexual power dynamics between these groups, with heterosexual men situated in more socially powerful positions than women and LGBTQ+ people. However, women and LGBTQ+ people also face non-sexual physical threats, such as death threats, in digital spaces due to their gender and sexual orientation (Younes 2021).[87] Threats against them are often related to their gender and sexual orientation through the inclusion of derogatory slurs shared alongside the threats of physical and sexual violence. Sexual and non-sexual online threats like these can be especially frightening and consequential for them because of the high rates of discrimination and sexual and physical violence women (World Health Organization 2021) and LGBTQ+ people[88] are subjected to. Digital threats cause real fear among these groups and have been linked to physical violence (Manjoo 2012).

Many LGBTQ+ people have their physical safety and lives threatened online on a regular basis.

Research, including that done by GLAAD, has shown that many LGBTQ+ people have their physical safety and lives threatened online on a regular basis (National Coalition of Anti-Violence Programs 2016; Human Rights Watch 2019; GLAAD 2022). Digital threats against LGBTQ+ people and activists have led to physical attacks and deaths, including those committed by state actors (Gritten 2022). In Latin American countries such as El Salvador, Guatemala and Honduras, LGBTQ+ people

87 See also http://webfoundation.org/docs/2020/03/WF_WAGGGS-Survey-1-pager-1.pdf.

88 See www.hrc.org/resources/sexual-assault-and-the-lgbt-community; www150.statcan.gc.ca/n1/daily-quotidien/200909/dq200909a-eng.htm.

are at ongoing risk of physical violence and death (Ghoshal 2020). A report out of Latin America found that at least 1,300 LGBTQ+ people were murdered in Latin America and the Caribbean in a five-year period, primarily in Colombia, Mexico and Honduras (Moloney 2019). In recent years in the United States, there have been multiple attacks on drag performers and mass shootings in gay clubs. In 2022, following a shooting in a gay nightclub in Colorado, GLAAD (2022) reported that a poll showed 48 percent of LGBTQ+ respondents fear for their personal safety because of the current transphobic and homophobic political climate, and 43 percent felt unsafe speaking about LGBTQ+ equality online using their real name. In Afghanistan, LGBTQ+ people have been criminalized and association with the LGBTQ+ community online or in person can lead to serious social, physical and legal harms, including violence by the Taliban (Akbary 2022).

Digital threats and other controlling behaviour can occur during a relationship to maintain power and control over women, and after a relationship has ended to punish and harm women for leaving the relationship.

People in abusive intimate partner relationships may face digital threats or coercive control from their partners in digital spaces. Intimate partner violence (IPV) in heterosexual relationships is highly gendered, with many studies showing that women are most vulnerable to the negative impacts of IPV (Citron 2014; Aikenhead 2021). Digital threats and other controlling behaviour can occur during a relationship to maintain power and control over women, and after a relationship has ended to punish and harm women for leaving the relationship (Dragiewicz et al. 2018; Woodlock et al. 2020). Unfortunately, the use of technology to threaten women in intimate partner relationships is on the rise. An Australian study about the connection between technology and domestic violence found that anti-violence practitioners observed a 74.4 percent increase in the use of technology by abusive intimate partners to threaten women between 2015 and 2020. This is especially concerning as they noted that the likelihood that a woman will be killed by her male partner is 11.36 times more likely if she has been previously threatened by them (Woodlock et al. 2020). Further, outside of an intimate partner relationship, men's feelings of sexual entitlement to cis and trans women can result in men threatening women who reject their sexual advances in digital spaces, as will be discussed in greater detail in the section below on unwanted communication. For example, a study in India and Pakistan found women received online threats when they did not respond to or rejected romantic advances from men (Vashistha et al. 2019).

Additionally, those who advocate online for gender (Vasudevan 2018; Kovacs, Padte and SV 2013) and LGBTQ+ equality (United Nations 2022) may receive threats online for discussing those rights publicly or simply for being women or LGBTQ+ people in straight or male-dominated fields and digital spaces (Aziz 2020). Women (Sallam 2018) and LGBTQ+ activists (Office of the Council of Europe Commissioner for Human Rights 2021; GLAAD 2022), politicians (Kraicer and Dhrodia 2021; Inter-Parliamentary Union 2016) and journalists (Barton and Storm 2014) face frequent threats of physical violence, death and sexual assault, especially if they are speaking about sexuality, gender or feminism (Palumbo and Sienra 2017; Yahaya and Iyer 2022). A UN report, *#JournalistToo: Women Journalists Speak Out*, stated "while both male and female journalists are exposed to violence and threats to their safety in retaliation for their work, attacks on women are gender-based and highly sexualized online and offline" (Khan 2021). TFV against women and LGBTQ+ journalists, human rights defenders and politicians will be discussed in more detail in a later section of this report.

Unsolicited Sexual Images

People of all genders and sexual orientations send unsolicited sexual images for a variety of reasons

and people have a variety of responses to receiving them (Oswald et al. 2020; Dietzel 2022). Research by Canadian scholar Christopher Dietzel (2022) and Australian scholars Anastasia Powell and Nicola Henry (2017) found that some unsolicited sexual images are wanted, particularly in the context of a sexual relationship, whereas others are interpreted as a form of harassment or abuse. Unsolicited images that are unwanted can be a form of image-based abuse (McGlynn and Rackley 2017). Unsolicited sexual images can be sent in a variety of contexts ranging from intimate partner relationships to complete strangers. For example, some unsolicited sexual images come in the form of spam or advertisements for sexual content and sexual services (Powell and Henry 2017).

Unsolicited images can be a form of TFGBV when they cause harm to the person receiving them. In an Egyptian study on TFV against women by Fatma Mohammed Hassan et al. (2020), unsolicited sexual images were one of the most common forms of TFGBV women experienced. The images in these cases were typically sent to women by an unknown person. In an international study on girls by Plan International, girls reported being sent unsolicited pornographic images in order to harass them (Goulds et al. 2020). An additional study on young adults in Sub-Saharan Africa found that receiving unwanted sexually explicit images was the most common form of TFV experienced by those surveyed (Makinde et al. 2021).

Clare McGlynn and Kelly Johnson's book *Cyberflashing: Recognising Harms, Reforming Laws* discusses the phenomenon of men who send unsolicited sexual images to women. Their study focused on women and girls in the United Kingdom, Ireland, the United States, Canada, Australia and Singapore (McGlynn and Johnson 2021). Their research focused specifically on men sending an image of a penis to women, which occurs in a variety of contexts. For example, a single picture may be sent to a single woman on a dating app, or multiple women may be sent the image using functions such as Apple's AirDrop to place the image on multiple women's phones (for example, groups of women collectively located in a public place such as public transit). McGlynn and Johnson found that "cyberflashing," the term they use for unsolicited sexual images, is often a form of gender-based harassment and that some women felt afraid, humiliated and violated by the act (ibid.).

Men's and women's reactions to unsolicited sexual images can be quite different. A study by Flora Oswald et al. (2020) found that women experienced more negative reactions to receiving these unsolicited sexual images than men. The intention behind why men and women send sexual images differs as well. Both women and men may send images to solicit sexual attention; however, men more commonly do it as a form of harassment. Oswald et al. (2020) found that men who engage in sending unsolicited sexual images can be motivated by misogyny and a desire to have power and control over women. In their research on unsolicited "dick pics," Rebecca Hayes and Molly Dragiewicz (2018) noted that there can be an element of aggrieved entitlement when men sent these unsolicited sexual images to women.

In a Canadian study by Dietzel (2022) about unsolicited sexual images, gay and bisexual men considered sending unsolicited sexual images (such as "dick pics") more socially acceptable and less harmful among men who sleep with men than when heterosexual women received the same images. This was in part because the gendered power dynamics are very different when same-sex people share photos with each other compared to when men send images to women. However, some men do still find the images harassing. In another study, Dietzel (2021) found that the highly sexualized nature of men's dating and hook-up practices, along with gendered assumptions about men's desire for sexual activity, including the pressure to send and positively respond to sexual images and sexual advances, contributed to rape culture on dating and hook-up apps.

NCDII

Of all forms of TFV, one of the most researched topics is NCDII. Early research on this subject was focused on young people and the risks of "sexting" (Karaian 2012), but research has expanded to adults, including women, men and members of the LGBTQ+ community. NCDII is now considered a form of what McGlynn and Erika Rackley (2017) have called "image-based sexual abuse," which is a subset of TFGBV. NCDII can range from sharing pictures through texts to livestreaming sexual images, including sexual assault, onto public social media or pornography sites without consent. In South Korea, there is a disturbing trend of hidden cameras being used to non-consensually capture nude and sexual images of women in public

bathrooms, change rooms and hotel rooms and distribute them on pornography sites and other places online (Aziz 2020; Ngyuen and Barr 2020). In some of the most severe cases of NCDII, images of women being sexually assaulted and raped have been livestreamed or posted online (Akhter 2018; Klein and Zaleski 2019; Oliver 2015).

Victims/survivors may have limited legal options in countries where sexuality, sexual orientation and women's bodies are highly regulated.

NCDII can cause significant harm to women and LGBTQ+ people living in countries where patriarchal and heteronormative standards are strictly enforced (Lirri 2015). Victims/survivors may have limited legal options in countries where sexuality, sexual orientation and women's bodies are highly regulated. A study on NCDII in Malawi and Uganda showed that laws against pornography and obscenity left victims/survivors of NCDII in a difficult position, as these laws are used to regulate women's autonomy, not protect them from perpetrators of NCDII (Chisala-Tempelhoff and Kirya 2016). Women in the images were often "slut-shamed" for consenting to be featured in the original images rather than provided help with the exploitative distribution of their private images. In Uganda, a female pop star whose images were posted online by an ex-intimate partner had some religious leaders call for her to be arrested and prosecuted for being featured in the images. In Asia, indecency, morality and obscenity laws have been used against women's sexual expression and advocacy (Padte and Kovacs 2013; Global Information Society Watch 2017; Kayastha and Baramu 2021). Additionally, police powers and laws restricting sexual expression/identity have been used in the Middle East and North Africa to prosecute members of the LGBTQ+ community who have been identified through gay dating apps and social media surveillance (Younes 2021; Akbary 2022).

Research has shown that women (Klein and Zaleski 2019) and members of the LGBTQ+ community (Waldman 2019) report higher pressure to share intimate images in digital spaces. In his research on gay online communities in the United States, Ari Ezra Waldman (2019) found that NCDII is more common in gay and bisexual communities, where there are heightened norms for disclosing intimate images, which can increase the risk of having the images shared without consent or used in abusive ways. For example, the research organization Data & Society reported that LGB+ people are more likely than heterosexual people to have had someone threaten to share their intimate images (Lenhart, Ybarra and Price-Feeney 2016).

Sharing an LGBTQ+ person's intimate images, which may identify their sexual orientation or sex assigned at birth, can put them at risk if they work or live in a community that holds homophobic and transphobic views, such as those mentioned above. Even in countries where same-sex relationships are not criminalized, homophobia and transphobia may still be common and can make LGBTQ+ people vulnerable when images that expose their sexual orientation or sex assigned at birth are shared without consent. In a well-known case in the United States, a young man, Tyler Clementi, died by suicide after unknowingly being filmed on a webcam kissing another man by his roommate, who showed the content to others at their university and publicly tweeted negatively about Clementi's sexual orientation (Fairbairn 2015).

A large quantitative and qualitative study on NCDII out of Australia, New Zealand and the United Kingdom by a group of researchers found that people's responses to having their images shared without consent varied: some had positive feelings such as flattery; others experienced relatively minor negative impacts; some felt serious disruptions in their lives; and others reported severe, ongoing, life-altering impacts (Henry et al. 2020). These researchers found that there were differences among the reactions depending on the genders and sexual orientation of the participants. Although men in the study reported higher prevalence of being victimized by NCDII, women, in particular LGB+ women, reported experiencing more negative harms related to their emotions, reputations, safety, health and relationships compared to men when their intimate images were shared without consent. LGB+ people, young people and members of racial or ethnic minorities experienced more

harassment due to NCDII. Men were more likely to take, share and threaten to share intimate images than women. LGB+ people were more likely to take, share and threaten to share intimate images than heterosexual people, which may be linked to the normalization of sexual image disclosure in those communities mentioned above. The researchers found that their data pointed "to a troubling trend where digital technologies are being used not only as a form of control, abuse and harassment, but as a further expression and consolidation of masculine entitlement and privilege, and as a tactic of sexuality-shaming women, women of colour or those identifying as lesbian, gay, bisexual, transgender, intersex or a non-binary gender" (ibid., 27).

In a study of Canadian NCDII criminal cases, Moira Aikenhead (2021) found that there was a "gendered double-standard" regarding the sharing of intimate images, with women being slut-shamed and blamed by some members of the public for taking the images in the first place. Offenders in these cases were cited as trying to humiliate the victim, and many images were posted on public websites such as dating or pornography websites. The vast majority of NCDII criminal cases in Canada involved female victims and male offenders.

Reports of NCDII increased during the COVID-19 pandemic. In Brazil, SaferNet reported that there was a 154.9 percent increase in cases of NCDII in April 2020 compared to April 2019 and that most of the victims reporting to them (70 percent) were women (Ramos 2020). The United Kingdom's Revenge Porn Helpline saw a spike in cases reported after the COVID-19 pandemic began (Ward 2021). Its report also showed a gendered difference in who was seeking help. Sixty-two percent of the 3,146 cases in 2020 were women and most perpetrators were men (84.5 percent). The quantity of images shared was also much higher for women than for men (ibid.). Victim blaming was a common theme across many countries' studies on NCDII (Sequera 2021; Ayres and Quevedo 2020; Giorgetti et al. 2016).

LGBTQ+ people are at significant risk of harms if they are in a country where it is not safe to be LGBTQ+ publicly, such as in countries where same-sex relationships are criminalized and gendered dress codes are enforced.

Additionally, the gendered nature of NCDII can be seen on websites and online groups that are dedicated to publishing "revenge porn" or the collections of non-consensually shared intimate images (*La Prensa* 2020). Studies have shown that these public websites dedicated to publishing nude and sexual images without consent primarily focus on women (Slane and Langlois 2016). A study by Carolyn A. Uhl et al. (2018) found that 92 percent of the profiles on these sites were of women. A study of these sites by Henry and Flynn (2019) found that 85 percent of images on one website featuring 12,450 profiles were of women and women's images were viewed more often than men's images, sometimes upwards of 100,000 times. Matthew Hall and Jeff Hearn (2019) examined the language used on these sites and found "power, control and (hetro)sexuality were the main underlying themes," and men were attempting to hurt or control the women in the images. According to Walter S. DeKeseredy and Martin D. Schwartz's (2016) male peer support theory, some men who non-consensually share sexual images in groups rely on patriarchal masculinity to justify their sexually abusive behaviour.

Blackmail

Gender and sexuality can play a significant role in blackmail online. GenderIT listed extortion as one of the 13 manifestations of TFGBV[89] and extortion was found to be a form of TFGBV in multiple studies, including those out of Palestine (Odeah 2018), Bangladesh (Akter 2018), Australia (Powell and Henry 2017), India and Pakistan (Vashistha et al. 2019), the United States (Lenhart, Ybarra and Price-Feeney 2016) and Europe (Council of Europe 2018). Blackmail is a particularly serious risk for many LGBTQ+ people, who may not share their sexual orientation and sex assigned at birth publicly due to privacy, safety and legal concerns.

LGBTQ+ people are at significant risk of harms if they are in a country where it is not safe to be LGBTQ+ publicly, such as in countries where same-sex relationships are criminalized and gendered dress codes are enforced.[90] Homophobia, transphobia and violence toward LGBTQ+ people exist in all countries, but in countries where same-sex relationships are criminalized, the risk is especially high (Akbary 2022). The International Gay and Lesbian Human Rights Commission report *Nowhere to Turn: Blackmail and Extortion of LGBT People in Sub-Saharan Africa* detailed how LGBTQ+ people in some African countries face physical and legal risks if their sexual orientation is exposed online or in their communities. Authors Ryan Thoreson and Sam Cook (2011) noted that, "in places where it is illegal, stigmatizing, or dangerous to identify as LGBT or to engage in same-sex activity, keeping one's sexuality a secret may be, quite literally, a matter of life or death." The report cited studies from Botswana, Cameroon, Ghana, Malawi, Namibia, Nigeria and South Africa where LGBTQ+ people reported incidents of blackmail related to their sexual orientation and gender identity. Details of their sexual orientation were sometimes gathered from their communications on the internet and used to blackmail them by threatening to expose their sexual orientation to their families and communities. This risk is felt by LGBTQ+ people in many other countries. For example, in Brazil, a record number of LGBTQ+ people have been killed, so their privacy is particularly important to them to avoid violence and death (TGEU 2021; Trevisan 2018). Extortion against LGBTQ+ people can also occur on a larger scale. In 2021, hackers obtained access to an Israeli gay dating website and posted the data online after the company refused to pay a ransom (France 24 2021).

Blackmail is a particularly serious risk for many LGBTQ+ people, who may not share their sexual orientation and sex assigned at birth publicly due to privacy, safety and legal concerns.

Sexual extortion is another common form of digital blackmail (Aziz 2020). Sometimes called "sextortion," it occurs when someone uses sexual images of another person to demand something from them, often additional sexual images or sexual contact, or to force someone to stay in an intimate relationship (Wittes et al. 2016; Wolak and Finkelhor 2016). Women and young people are at particular risk of sextortion; however, an American study on sextortion of adults during the COVID-19 pandemic found that men were increasingly targets of sextortion, along with Black and Indigenous women, and LGBTQ+ people (Eaton, Ramjee and Saunders 2022). Intimate images that were originally shared consensually, images that were taken without consent or images that were hacked or stolen can be used in sextortion. Women in Mexico reported an increase in the use of sexual images to extort and harm them during the early stage of the pandemic (*El Heraldo* 2020). Gendered extortion can occur in other contexts. Women in India and Pakistan reported being blackmailed by men who had their phone numbers (not sexual images) and threatened to publish their contact information and false information about them if they did not continue speaking with them (Vashistha et al. 2019).

89 See https://genderit.org/resources/13-manifestations-gender-based-violence-using-technology.

90 See www.ohchr.org/en/sexual-orientation-and-gender-identity/about-lgbti-people-and-human-rights.

In a US study of 152 sextortion offenders, Roberta O'Malley and Karen Holt (2022) defined four main types of sextortion: sextortion that targeted minors; sextortion involving a cybercrime (where images were hacked, stolen or obtained through deceit); sextortion conducted by a current or ex-intimate partner; and transnational sextortion. In cases where minors were targeted, which were the most common (52.6 percent) and often involved grooming the victims, 100 percent of the offenders were men, 71.3 percent of the victims were female, 88.8 percent of the victims were minors and 100 percent of the demands were sexual. In cybercrime cases (21.1 percent), 96.9 percent of the offenders were men, 93.8 percent of the victims were female, 28.1 percent of the victims were minors and 84.4 percent of the demands were sexual. In cases involving intimate partners (12.5 percent), 100 percent of the offenders were men, 94.7 percent of the victims were female, 26.3 percent of the victims were minors and 36.8 percent of the demands were sexual. In cases of transnational sextortion (11.2 percent), where victims are more commonly extorted for money, 58.5 percent of the perpetrators were men, 5.9 percent of the victims were female, 5.9 percent of the victims were minors and none of the demands were sexual (they were more often financial).

Women and LGBTQ+ people face high levels of unwanted contact in the form of sexual harassment and unwanted requests for romantic and sexual encounters.

Repeated Unwanted Contact

Repeated unwanted contact, sexual or otherwise, can cause distress in some circumstances, can be intimidating in others or can be as serious as stalking, which can cause ongoing distress and fear and pose a legitimate risk to the target's physical safety.

Women and LGBTQ+ people face high levels of unwanted contact in the form of sexual harassment and unwanted requests for romantic and sexual encounters. A study on online sexual harassment in Bangladesh found that women commonly received unwanted sexual propositions and inquiries about dates (Nova et al. 2019). In other studies, in India, Pakistan (Digital Rights Foundation 2017a) and Sub-Saharan Africa (Makinde et al. 2021), researchers found similar results, with women reporting that they were repeatedly contacted by people proposing or demanding a sexual relationship with them (Ramaseshan et al. 2019). Sexual harassment is reported as a form of TFGBV in the majority of the studies reviewed for this report, with women experiencing more sexual harassment than men (Powell and Henry 2015).

A 2016 American study on online harassment by the Pew Research Center found that men are more likely to receive threats of physical violence, but women are more likely to experience sexual harassment. In the study, people's gender, religious identity and sexual orientation were common reasons for the sexual harassment (Duggan 2017). In 2021, the Pew Research Center found women were more likely to be harassed and to say the reason they were harassed was because of their gender (Vogels 2021). An Australian study by Powell and Henry (2015) shows that women are more likely to experience sexual harassment, particularly by men. The gendered nature of sexual harassment was shown in multiple studies, including those in Egypt (Zagloul et al. 2022), Ghana (Media Foundation for West Africa 2017), Kenya (African Development Bank Group 2016), Pakistan (Hassan, Unwin and Gardezi 2018) and India (Vashistha et al. 2019), where gender norms were often strictly enforced by families, the media and society, and the normalization of male dominance was a common feature of digital sexual harassment against women.

LGBTQ+ people also reported unwanted and inappropriate sexual requests because of their gender identity and sexual orientation (Dietzel

2021; Udwadia and Grewal 2019). Transgender people, especially women, reported being sexually objectified and fetishized on dating apps and that they have been made to feel unsafe by that contact in those digital spaces (Albury et al. 2021). A qualitative study in India by Point of View found that LGBTQ+ people receive unwanted messages asking inappropriate questions about their bodies and demands for sex (Udwadia and Grewal 2019).

Further, repeated unwanted contact can amount to stalking. Stalking is one of the most serious forms of TFGBV — it is the repeated contact or surveillance by another person that causes a person to feel fearful. It can be related to IPV and men's feelings of entitlement toward women online (European Institute for Gender Equality 2017); however, women and LGBTQ+ individuals are also stalked online due to their gender identity, sexual orientation and leadership positions by strangers and people they know online (Curlew and Monaghan 2019). Stalking has been linked to in-person sexual and physical violence (FRA — European Union Agency for Fundamental Rights 2014; Sambasivan et al. 2019).

The Pew Research Center examined Americans' experiences with online harassment in 2016 and 2021 and found that women are more likely to be cyberstalked compared to men (Duggan 2017; Vogels 2021). Statistics Canada reported that women are more likely to be cyberstalked than men, a number that increases for young women (Burlock and Hudon 2018). In Malawi, women reported being stalked online as the most common form of TFGBV they faced, which made them feel unsafe, fearful, distressed or alarmed (Malanga 2021). Cyberstalking was also the most common form of TFGBV experienced by women in a study from Bangladesh, India and Pakistan, with 66 percent of women participants reporting being stalked online (Sambasivan et al. 2019). However, the gendered aspect of stalking was not consistent in all studies. A study on Sub-Saharan Africa did not find a gendered difference in stalking among genders (Makinde et al. 2021).

AirTags have been used to track women when their male ex-partner places them in items belonging to their children.

Intimate partners are often the perpetrators of stalking. Research by Diana Freed et al. (2018) documented some of the ways current and ex-intimate partners use technology to stalk their targets.[91] When a person is still in the relationship, the abusive partner may have physical access to the other person's device and can use that access for surveillance purposes. The abuser may also own the device, share an account with their partner and/or control access to their partner's device and its contents. This limits the person's freedoms and their ability to seek out help. Further, the abusive partner may give their shared child(ren) a device to stalk their current or ex-partner. For example, Apple AirTags have been used to track women when their male ex-partner places them in items belonging to their children (Cole 2022). Further, former and current abusive partners may have access or knowledge of their target's accounts, private information and photographs that can be used to facilitate the stalking. Delanie Woodlock (2017) reported that intimate partner stalking against women can lead to feelings of isolation, omnipresence and constant surveillance that can be extremely disruptive to their lives and cause ongoing fear.

More complex forms of technology have also been used to stalk intimate partners. Abusive partners may install spyware on their victim's phone to track them (Thomasen and Dunn 2021). This technology allows the abusive partner to monitor the activity of the other person, including their texts and online interactions, and, in some cases, can be used to turn on the person's microphone or camera to observe their activity. These apps have been marketed to facilitate gender-based stalking. As noted by CitizenLab, stalkerware spyware has been marketed as an intimate partner tracking app,

91 See also Havron et al. (2019).

and many comments on apps sold to track intimate partners are about tracking women in particular (Khoo, Robertson and Deibert 2019). Smart home technology, such as alarm systems and listening devices (Lo 2021), and drones (Thomasen 2018), have also been used to stalk and harass women.

Organized groups can also be engaged in stalking women and LGBTQ+ people. For example, research by Abigail Curlew and Jeffrey Monaghan (2019) described a website dedicated to stalking and sharing private information about transgender people, in particular women and neurodivergent people. According to Curlew and Monaghan, this site uses crowdsourcing to collect information to create "dossiers" on the website that purposely misgenders transgender people and posts their pre-transition photos and deadnames, along with discriminatory commentary about them. In 2022, actors from this website targeted a transgender Canadian woman, Clara Sorrenti. They engaged in an organized, hate-filled online harassment campaign against her, including doxing her. Someone made a false report to the police — a practice known as swatting (Khoo 2021) — that she had killed her mother and was going to go to city hall and kill cisgendered people (Farokhmanesh 2022). Armed police showed up at her house to arrest her. After users from this website identified her location, Sorrenti fled the country for her safety.

Unauthorized Access

Unauthorized access to a person's personal devices or online accounts is linked to stalking, harassment and NCDII. A 2020 study by the BC Society of Transition Houses demonstrated how common experiencing this type of behaviour was for victims of gender-based violence. It found that 85.29 percent of victim service workers worked with women who had their social media platforms hacked and monitored by an abuser, 79.41 percent had worked with women whose mobile phone was hacked and monitored by an abuser, and 75.47 percent had worked with women whose email had been hacked and monitored by an abuser.

Karen Levy and Bruce Schneier (2020) have noted that intimate partners have unique access to the personal information of their partners, including knowing their passwords or the information needed to gain access to their passwords, which allows them to access a person's account without consent. Once access is gained, this information can be used to track a person's communication and whereabouts. In an Australian study by Heather Douglas, Bridget A. Harris and Molly Dragiewicz (2019) about women's experiences with technology and domestic violence, some participants reported that their abusive partners maintained unauthorized access to their accounts and at times changed their passwords, so they no longer had access to their accounts. In other cases, keyloggers were installed on women's devices, allowing their abusive partners to access their passwords and communication. Additionally, hacking has also been used as a technique to obtain sexual photos of people to extort them (O'Malley and Holt 2022). Many women are forced to provide access to their accounts and devices by male partners or family members, as discussed in the next section.

Outside of intimate partnerships, human rights defenders and women's and LGBTQ+ organizations are also at risk of unauthorized access by abusive individuals who oppose their work (Acoso 2020).

Monitored, Tracked or Spied On

Many women and LGBTQ+ people have their devices and accounts monitored by family members, current or former intimate partners and malicious actors. In particular in countries where same-sex marriage is illegal, as mentioned above, social and state surveillance of women and LGBTQ+ people puts them at risk of violence and persecution (Akbary 2022).

As noted in the section on unauthorized access, intimate partner monitoring is a common problem. A study in Brazil noted that among young people, adolescent boys and young men monitoring, tracking and stalking their girlfriends on mobile phones was a normalized practice (Lopes Gomes Pinto Ferreira 2021). In some countries, there is also a significant amount of monitoring done by family members. In Pakistan, it is common for women's phones to be controlled and monitored by male family members (Jamil 2021). Gender inequalities, in particular in conservative and religious families, contribute to this practice. In a study in Sub-Saharan Africa, 18 percent of the study's participants reported being spied on with a camera or listening device, or tracked using a location tracker, such as GPS; however, information on who was spying on them was not collected (Makinde et al. 2021, 95). That research noted that in Uganda, two women were killed by their partners after they

allegedly found romantic messages from someone else on their phones (ibid., 87). In Pakistan, four women were killed when a video appeared online showing them clapping and singing at a wedding (Aziz 2020, 34).

Many women and LGBTQ+ people have their devices and accounts monitored by family members, current or former intimate partners and malicious actors.

Family surveillance was also commonly found in India, where girls' phones were more likely to be monitored and controlled by family members than boys' (Villamil 2022). This surveillance and lack of access to technology can be especially restricting for LGBTQ+ women and disabled women, who may have limited cultural and physical freedoms (Radhakrishnan 2020). A study in Palestine found that surveillance is conducted by people in society who observe online interactions, including family members who "friend" and monitor women's interactions online, impacting how freely women can communicate in digital spaces. In some cases, apps are installed on women's phones by family members to track their location and communication under the guise of protecting them (Odeh 2018). Additionally, fear of political persecution limited how freely women could communicate online.

In India, rules in certain rural and conservative communities banned young people, in particular unmarried women and girls, from using chat apps and mobile phones altogether (Kovacs 2017). In less common cases, married women were banned or restricted from using mobile phones by their husbands and families. Those who disobeyed the rules could face financial or social punishments and community members were encouraged to report girls who disobeyed the rules.

Research by the Internet Democracy Project found that many of the concerns expressed by conservative leaders were focused on controlling women's sexual and romantic choices (ibid.). However, these bans limit women's autonomy in many ways beyond their romantic and sexual choices. They can affect their freedom of communication and their ability to seek help and access information, as well as their personal development. In some cases, those who did have access to phones were limited in the places and ways they could use them. A study by Giorgia Barboni et al. (2018) found that economic and normative barriers limited women's access and freedom in relation to mobile phones, sexist concerns about women's sexual purity, reputation and family responsibility. Community members often made judgments about the purity of girls who used mobile phones in public spaces (ibid.).

Family, community and state surveillance of women was also reported in research out of Morocco, Egypt, Saudi Arabia and Pakistan: In Egypt, several women were arrested for speaking out about sexual assault online. In Saudi Arabia, an online video of a woman wearing a miniskirt led to calls for her to be arrested. A Palestinian woman was killed in 2019 after her family found photos of her with her fiancé on social media (Abdullah and Campbell 2021). In Pakistan, the Digital Rights Foundation (2017b) found that female journalists were being monitored by the state, intelligence agencies and social actors and experienced harassment due to their work. Additionally, surveillance of the LGBTQ+ community in the Middle East and North Africa has led to arrests and state-sanctioned violence (Younes 2021).

Doxing

The term "doxing" (sometimes spelled "doxxing") comes from the practice of "dropping documents" online (Sobieraj 2017). It usually refers to having personal information, such as a person's contact information or address, posted online without permission. In a study on TFGBV, one woman reported having her home address, details of the interior of her house and photos of her car posted online to intimidate her (ibid.). Doxing is used in a variety of harmful manners, including threats to publish private information to silence people and doxing as a controlling form of abuse or punishment (Anderson and Wood 2021).

Doxing is often used to increase harassment against a person by providing additional ways for harassers to contact them and can cause increased fear for a person's physical safety when their physical location is exposed online (Dunn and Petricone-Westwood 2018). In a study of Australian and UK adults, Henry et al. (2020, 27) found that in cases of NCDII, a person's identifying information, such as their name, contact information and social media accounts, was often posted along with the intimate image, encouraging additional harassment against them. As noted above, LGBTQ+ individuals are often doxed when people are trying to expose their sexual orientation and gender identity in harmful ways.

Doxing has a gendered element to it. A study involving women and men in Canada, Finland, Germany, Switzerland and the United States found that women were doxed in relation to being outspoken in male-dominated digital spaces (Eckert and Metzger-Riftkin 2020). In a study about Muslim women human rights defenders, several had their personal information doxed (Yahaya and Iyer 2022). Some women choose to communicate and do advocacy work online anonymously due to the risks associated with it, so keeping their personal information private is an important safety practice.

Networked Harassment

Alice E. Marwick and Robyn Caplan (2018) describe networked harassment as a form of collective online harassment that originates from a network of people with a shared agenda or world view. As will be discussed in another section of this report, women and transgender and gender-diverse journalists (Posetti et al. 2021), human rights defenders (Van Der Wilk 2018), politicians (Dhrodia 2018), and public figures (Gurumurthy and Dasarathy 2022; Marwick 2017) are subject to significant networked harassment. Investigative journalists such as Rana Ayyub from India (United Nations 2018) and Maria Ressa from the Philippines (Posetti 2017), have faced large-scale gender-based attacks, including threats of death and sexual violence. Hashtags such as #ArrestMariaRessa and a sexual deepfake of Ayyub spread across WhatsApp and Twitter were used to drive harassment toward them. Hashtags, derogatory sexist comments and sexual threats have been used against journalists in Latin America as well (Cuellar and Chaher 2020). Many of these women journalists were targeted with networked harassment for criticizing their governments or discussing feminist issues.

In Marwick and Caplan's (2018) article on networked harassment, they focus on gender-based harassment against women originating from what is known as the "manosphere." Proponents of the manosphere blame feminism for what they perceive as a negative shift in society that no longer embraces patriarchal and heteronormative ideals. One of the first large-scale online harassment campaigns, #Gamergate, was conducted against several female gamers by male gamers who felt that the gaming industry was threatened by these women's engagement in the gaming industry. Their campaign against these women resulted in a nearly decade-long harassment campaign.

Lies and disinformation campaigns about individual women and women as a group are used to reinforce sexist gender norms.

The manosphere is often connected with the alt-right in the West. Members of the alt-right espouse white nationalism, homophobia, transphobia and misogyny and have a particular dislike of feminists (Massanari 2018). Those with a large following can drive significant gender-based violence toward particular women when they criticize them on their platforms (Brown, Sanderson and Ortega 2022). These disinformation campaigns will be discussed in further detail below.

False Information

Lies and disinformation campaigns about individual women and women as a group are used to reinforce sexist gender norms. In 2023, the United Nations' 67th Commission on the Status of Women noted that "the way many digital platforms are designed, maintained and governed has given

rise to disinformation, misinformation and hate speech, which can undermine the fulfilment of women's and girls' rights, including the right to freedom of opinion and expression and to participate in all spheres of public life" (UN Women 2023a, para. 40).

A Wilson Center report showed that gendered and sexualized disinformation online is a unique form of gendered abuse that involves sexist, racist, transphobic and sexual narratives, with sexual narratives being the most common (Jankowicz et al. 2021). In its research, the Wilson Center found that racialized women faced intersectional attacks that targeted their race and gender. In another study, Sarah Sobieraj (2020) found that women who were in male-dominated fields such as politics and/or spoke about feminist issues, were particularly targeted — again, racialized women experienced some of the most severe attacks. Demos reported that gendered disinformation is used to silence influential women in digital spaces (Judson et al. 2020). It applies sexist norms to these women and spreads lies about them, including doctored sexual images of them. Research by Samantha Bradshaw and Amélie Henle (2021) shows how gendered disinformation campaigns against feminism and women's rights were orchestrated by state-sponsored accounts from Iran, Russia and Venezuela, with high-profile feminists commonly targeted.

Similar disinformation campaigns are made against LGBTQ+ people (Strand and Svensson 2021). These campaigns often falsely claim that LGBTQ+ people are a threat to children because they are sexual predators and that their "gender ideology" is a threat to the social fabric. In one study, this behaviour was found to be particularly common in the Philippines and Poland. In Brazil, anti-feminist, anti-LGBTQ+ and anti-human rights campaigns have led to violence against these groups (Sívori and Zilli 2022).

Defamatory and false information about women and LGBTQ+ people's sexual practices are typically used to discredit them (Bartow 2009). In 2020, 165 Pakistani women journalists released a statement that said they were discredited by political parties and opponents, some of whom suggested the women journalists had personal relations with politicians of other parties and accused them of taking bribes to promote political agendas.[92] A major problem for women in Asia was the dissemination of false information, including reports of men falsely claiming women were sex workers (Aziz 2020). In some cases, abusers have made fake websites that spread lies about their ex-partner in order to ruin their reputations online (Dunn 2020b). More details on the ways that fake information harms women and LGBTQ+ people will be discussed in the following sections on impersonation and identity-based harms.

Impersonation

Impersonation, such as the use of fake profiles, is used as a form of gender-based violence and violence against LGBTQ+ people (Aziz 2020). Fake profiles can be used by abusive intimate partners to gain information about their ex-partner by posing as them and communicating with family members, friends or co-workers to get them to disclose information (Cox 2014). In an international study on TFGBV against women, The Economist Intelligence Unit reported that 63 percent of participants said they had been impersonated online.[93] In a study from Southeast Asia, 15 percent of cis and trans women participants had been impersonated; it was more common among those who were lower income, younger or sexual minorities, and fake sexual images were made of women and posted on the fake profile of them (Sambasivan et al. 2019).

Fake profiles have been used to humiliate women and LGBTQ+ people by posting inappropriate content from the fake profile featuring them (Waldman 2019; Dunn 2020b). Some people have hacked into other people's profiles and manipulated their existing profiles, while others have created new fake profiles. These fake profiles have included sexual content that suggested the people were engaged in sexual activities that they had not engaged in or that they were interested in such activity. This type of impersonation can lead to physical harm. A study on criminal NCDII cases in Canada by Aikenhead (2021) found fake online profiles suggesting that the person is available for unwanted sexual encounters, including "rape fantasies" and escort services, have led to ongoing unwanted messages requesting sexual contact, as well as physical and sexual assaults. In the United

92 See https://docs.google.com/document/d/1DD8BQ53noKO6zHy-gysGnFjeKT4ride4uYtQsNNRYoc/edit.

93 See https://onlineviolencewomen.eiu.com/.

States, a gay man created multiple fake profiles of his ex on Grindr, leading to hundreds of men unexpectedly coming to his ex-partner's home and workplace demanding sex with him (Goldberg 2019).

Fake profiles can also be used to make it seem that a person is saying something that they would not have said online to smear their reputations (Dunn 2020a). For example, in the case of investigative journalist Rana Ayyub mentioned earlier, a fake Twitter profile of her was used to say she supported child rape and hated Indians, which contributed to the networked harassment against her (Citron 2019).

Identity-Based Harassment and Discrimination

Digital identity-based harassment and discrimination occurs when a person is targeted because they are a member of an equity-seeking group. They face attacks directly because they are a woman, LGBTQ+ person, religious, disabled or a member of an ethnic group, or Black, Indigenous or a person of colour.

Gender identity is one reason why a person can be discriminatorily targeted by TFV. Women are targeted because of their gender more than men and patriarchal norms are reinforced online in these attacks (Vasudevan 2018). Like all forms of gender-based violence, gender inequality, misogyny and patriarchy are the root of much TFGBV against women (Aziz 2020). Gendered attacks also focus on women's other identity factors such as sexual orientation, gender identity, gender expression, race and class (Iyer, Nyamwire and Nabulega 2020). In India, the colour of a woman's skin and her caste can alter the type of TFV she faces. As noted by Kiruba Munusamy (2018), "unlike online violence that privileged women face which are most often only sexual, the violence that underprivileged outcaste, dark-skinned, minority women experience are intersectional, extreme, unique and invariably high as they are hateful and identity-based aiming to defame, humiliate, delegitimise or undermine an individual." In her book *Misogynoir Transformed: Black Women's Digital Resistance*, Moya Bailey (2021) discusses the way stereotypes such as the Jezebel, mammy or Sapphire are evoked online to dehumanize Black women. She calls the form of discrimination Black women face online "misogynoir," which she defines as "the anti-Black racist misogyny that Black women experience, particularly in US visual and digital culture" (ibid., 1).

Like all forms of gender-based violence, gender inequality, misogyny and patriarchy are the root of much TFGBV against women.

Other identity factors can intersect with women's identities to impact the TFV they experience. Shia Muslim women in Pakistan are targeted because of their gender and their religion (Anwer 2022). As noted by Pollicy and Musawah, Muslim women human rights defenders who push back against patriarchal norms face unique risks related to their religion when they engage online (Yahaya and Iyer 2022). Outspoken women in Egypt have been targeted online because of their religion, gender, culture and race (Sallam 2018). Culturally and linguistically diverse women in Australia reported specific threats related to their social location, including threats of deportation for those without citizenship and honour killings (Louie 2021; eSafety Commissioner 2019). Indigenous women in Canada, who have some of the highest reports of gender-based violence in the country, experience forms of TFV, such as human trafficking and online hate, that are connected to sexist and colonial oppression against them (Bailey and Shayan 2016). These examples demonstrate the intersectionality of identity-based harassment and discrimination in digital spaces.

Within the LGBTQ+ community, people are targeted because of their sexual orientation, gender identity and gender expression. According to Sobieraj (2017), women of colour and LGBTQ+ people are exposed to racist, transphobic and homophobic slurs online related to their intersecting identities. Attacks are focused on their physical appearance, sexual orientation and sexual activity. These attacks also challenge their capacity to be in leadership roles and threaten physical and sexual violence. A study by Brandwatch (2019) analyzed 10 million posts

from the United Kingdom and the United States about transgender people, finding a significant number of transphobic posts. The study found that transgender people face daily attacks and comments on their timeline, including comments that are linked to their race. In the most severe cases, there were calls for transgender genocide. Brandwatch found that abusive content often spiked when laws and policies about trans rights were proposed by governments. In Pakistan, for example, despite the introduction of a transgender rights bill in 2018, transgender people faced death threats and at least 20 transgender people were murdered in 2021 (Zaman 2022).

Online platforms themselves can contribute to the marginalization of LGBTQ+ people. On many digital platforms, there are limited gender options that do not allow transgender or gender-diverse people to properly express their gender identity, which can cause them harm (Lui, Singh and Giuga, forthcoming 2023). Research by Kath Albury et al. (2021) found problems with the structure of dating apps. Most dating apps are not designed to be inclusive or safe for transgender people, and often do not even provide a space for them to authentically define their gender identity. Florence Ashley's (2018b) research discusses the abuse that transgender people face, including accusations of gender fraud.

As noted earlier, LGBTQ+ people are targeted online because of their sexual orientation. A study by the Australian eSafety Commissioner found that LGBTQ+ people experienced double the amount of hate speech (30 percent) compared to the national population (14 percent). A report by ADL (the Anti-Defamation League) Center for Technology and Society (2021) found that 64 percent of LGBTQ+ respondents reported experiencing online harassment compared to 41 percent of the general population. A study of people in Australia, New Zealand and the United Kingdom showed that LGBTQ+ people experience more negative impacts from online harassment than heterosexual people (Powell et al. 2020). Their intersecting identities can influence the discrimination they face. Research by Andrew Farrell (2021) has shown that Indigenous LGBTQ+ people can face discrimination on dating apps based on their Indigenous identity. In countries where same-sex relationships are criminalized or considered socially unacceptable, LGBTQ+ people can be monitored, blackmailed and harassed online (Thoreson and Cook 2011). Some have been prosecuted by the state and even killed (Human Rights Watch 2020; Sallam 2018; Gritten 2022). Privacy online is therefore extremely important to the LGBTQ+ community. Rebecca Ryakitimbo (2018) has written about the importance of data and privacy in Tanzania, where the government has created a task force to identify digital content about gay people to prosecute them.

There are growing online movements against feminists, LGBTQ+ people and human rights defenders more generally where their identities are attacked as a group.

As mentioned in the networked harassment section, there are growing online movements against feminists, LGBTQ+ people and human rights defenders more generally where their identities are attacked as a group. This has been seen in Brazil, where discriminatory views have been advanced by the public and political leaders, including the country's previous president, Jair Bolsonaro, and adopted by large portions of the broader population (Sívori and Zilli 2022). These online movements have been linked to the deaths of human rights defenders, including a Black bisexual councilwoman, Marielle Franco (Kaul 2021; Judson 2021).

Within the Western manosphere, there are groups of men, called incels (a term meaning "involuntary celibate"), who feel entitled to sex with women, and who organize online against women's rights to sexual autonomy. According to Stephane J. Baele, Lewys Brace and Travis G. Coan (2019), incels are largely groups of men, linked to men's rights activism (Boyd and Sheehy 2016) and the manosphere (McCulloch et al. 2019; Guy 2021), who hold an extremist world view, believing they are entitled to sex with women and supporting

patriarchal monogamy. Many hold particular hatred for racialized women and feminists. Ann McGinley (2022) reported that the most extreme incels advocate for the torture, rape and murder of women. This group's ideology and influence has been linked to violent incidents such as the 2018 van attack in Toronto, Canada, that killed 10 people, eight of whom were women, and injured others.

Background: Impacts of TFGBV and TFV against LGBTQ+ People

TFGBV and TFV against LGBTQ+ people have damaging results. The International Center for Research on Women has noted that TFGBV "can have severe and far-reaching psychological, physical, social and economic impacts on the lives of victims/survivors and their families" (Hinson et al. 2019). Studies have shown that women, girls and LGBTQ+ people who were targeted with TFV often experience more severe mental health impacts, feelings of fear and concerns for their physical safety compared to men.[94] For some, TFV has been linked to physical harms, even death (Ghoshal 2020; Human Rights Watch 2020; Gritten 2022). The harms victims/survivors experience within and beyond digital spaces are often minimized.

The impacts of TFV are wide and varying. A study of TFGBV against women in Malawi showed that perpetrators intended to harm women socially, psychologically, economically and physically. Many women responded to the abuse by blocking their attackers or leaving the platform altogether, leading to a silencing of many women online (Malanga 2021). This silencing effect has wider implications on freedom of expression, democracy and personal autonomy. A study in South Asia showed that women who had been cyberstalked, impersonated and had their nude images released without consent experienced reputational, emotional and physical harms, as well as coercive romantic involvement and self-censorship and limited digital participation (Sambasivan et al. 2019). This results in limitations to women's autonomy and freedoms.

TFV can also cause economic impacts for victims/survivors: some women have lost their jobs because of content that was posted about them online by abusers, it can be expensive for victims/survivors to replace devices or accounts that have been compromised, additional security tools may be needed, and ongoing mental stressors can negatively impact a person's professional capacity (Jane 2018; Citron 2014). These economic impacts add to the already unequal economic position many women and LGBTQ+ people face.

There are also larger systemic harms from TFGBV and TFV against LGBTQ+ people. Systemic issues include the reinforcement of sexist, homophobic, transphobic, racist, ableist and colonial norms, as well as the silencing of people who discuss feminism, LGBTQ+ rights, sexual and reproductive rights, anti-racism and other equality-focused topics (Palumbo and Sienra 2017). This can cause digital environments to be unsafe and create hostile environments for many people, driving them away from online discussions. One of the most disturbing impacts of TFV is the silencing of women, LGBTQ+ people and other marginalized individuals (Lodhi 2018; Iyer, Neema and Nabulega 2020). Plan International found that young women and girls faced TFV for speaking online about issues such as race, sexuality and disabilities, causing them to be fearful about speaking up (Goulds et al. 2020). Many are having to choose between tolerating the abuse that comes with speaking about their communities' interests online, or being silent. For some, the risks are just too high and they do not have the ability to express themselves freely without being subject to TFV. These impacts are unacceptable and require multisectoral responses to end them.

Some groups of people have been shown to experience particularly high levels of TFV compared to the general population of women and LGBTQ+ people. The following two subsections highlight the impacts of TFV on young people and journalists, human rights defenders and politicians, as they face particularly high rates of TFV compared to the general population and, as such, are unique populations that require additional analysis.

Young People

Previous research has shown that young people experience higher levels of TFV than older people (Duggan 2017; Vogels 2021). Several reports on the broader population have shown that young people are more likely to be attacked in digital spaces than older people. Reports on online harassment

94 See, for example, Powell et al. (2020); Lenhart et al. (2016); Vogels (2021).

in the United States by the Pew Research Center showed that young people were at higher risks of TFV, including threats for young men, and stalking and sexual harassment for young women (ibid.). A study from India showed that young people are at an increased risk of TFV, with significant impact on their mental health and well-being (Maurya et al. 2022). The US research institute Data & Society also found that young people were more likely to experience harassment and abuse online (Lenhart et al. 2016). Similar results were found in Australia (Powell and Henry 2015). A Statistics Canada study showed that young women were more likely to be stalked online in Canada than older women (Burlock and Hudon 2018).

Additional reports that focus on young people's experiences show high rates of TFV among that age group. An international survey by the World Wide Web Foundation and the World Association of Girl Guides and Girl Scouts reported that 52 percent of the young women and girls they surveyed faced online abuse.[95] Plan International also found significant rates of girls reported receiving threats and harassment online, with more than half of the girls surveyed reporting being harassed and abused online (Goulds et al. 2020). It is clear that special attention needs to be given to young people when considering how to address TFV.

Journalists, Human Rights Defenders and Politicians

There is a shockingly high amount of TFV aimed at journalists, human rights defenders and politicians. These people play a key role in democratic expression and can bring attention to gender, sexual orientation, race and other equality issues that are essential to the fight for justice for these groups (Jansen Reventlow 2017). Yet they may face unacceptable levels of TFV.

Many women and LGBTQ+ journalists, human rights defenders and politicians are exposed to regular incidents of TFV. There have been multiple reports on the negative gendered nature of TFV against women journalists. The Digital Rights Foundation (2019), UNESCO (Posetti and Shabbir 2022), the International Centre for Journalists (Posetti et al. 2020), International Federation of Journalists (2017), Reporters Without Borders (2018a; 2018b), International Women's Media Foundation (Barton and Storm 2014), Media Matters for Democracy (Lodhi 2018) and TrollBusters (Ferrier 2018) are all examples of organizations that have reported on this problematic trend.

A 2020 survey of more than 900 journalists in 125 countries by UNESCO and the International Center for Journalists showed that 73 percent of women journalists had experienced some form of TFV related to their work (Posetti et al. 2020). Twenty-five percent had been threatened physically and 18 percent had been threatened with sexual violence, including 13 percent receiving threats against people who are close to them. Eight percent were doxed. Certain topics appeared to generate higher levels of attacks: gender (47 percent), politics and elections (44 percent), and human rights and social policy (31 percent). Seventeen percent reported feeling physically unsafe due to the TFV. Many reacted by self-censoring what they discussed on social media (30 percent). Four percent quit their jobs due to the TFV they experienced. Another report by the same organizations stated that some women journalists were told to "toughen up" and learn to deal with the attacks against them as part of their job (Posetti and Shabbir 2021).

Abuse causes significant challenges for women journalists who may struggle with whether to stay in the profession or not due to safety concerns.

A report by Reporters Without Borders (2018b) found that some women who had reported on gender-based issues were even at risk of violence leading to death. Women journalists who reported on these issues experienced TFV, verbal and physical attacks, imprisonment and murder. Forty percent of the women surveyed reported

95 See http://webfoundation.org/docs/2020/03/WF_WAGGGS-Survey-1-pager-1.pdf.

being harassed online. Online abuse included doxing, sexist name calling, physical threats, networked harassment and censorship. Eleven of the reporters addressed in their study had been killed in relation to their work, including journalists in Afghanistan, India, Iraq and Mexico. This abuse causes significant challenges for women journalists who may struggle with whether to stay in the profession or not due to safety concerns. Silvio Waisbord (2020, 1033) has reported that journalists who have physical markers that identify them as being part of an equity-seeking group such as "gender, race, ethnicity, sexuality, and religion" may be at increased risk.

Women politicians are also exposed to higher rates of TFV and abuse in general (Inter-Parliamentary Union 2016). The Amnesty International (2018) report *#ToxicTwitter* studied the abusive tweets women politicians, activists and writers faced on Twitter. The report found that platforms such as Twitter are important spaces for women's voices to be heard, but that Twitter could be a toxic place for women. For example, among women members of Parliament (MPs) in the United Kingdom, one Black female MP, Diane Abbott, received almost half of the abusive tweets targeted against women MPs during the period the report reviewed. Women wanted to be on Twitter but found that speaking about gender, race and politics could trigger abuse on that platform and led many to self-censor.

Those advocating for feminist values, gender equality, reproductive rights, sexual expression and LGBTQ+ rights and against sexual violence are exposed to TFV related to their work.

The *#ToxicTwitter* report found that women's rights activists were also targeted with abuse on Twitter. Women who spoke up about anti-Black racism, reproductive rights and gender issues were threatened online (ibid.). Attacks often zeroed in on the woman's other identifying factors such as her race, sexual orientation, gender identity, disability or religion. Activists across the globe face this type of TFV. APC,[96] the World Wide Web Foundation,[97] the Middle East Institute,[98] GenderIT[99] and IT for Change[100] have all reported on the experiences of TFV activists online. Those advocating for feminist values,[101] gender equality,[102] reproductive rights,[103] sexual expression and LGBTQ+ rights,[104] and against sexual violence,[105] are exposed to TFV related to their work.

LGBTQ+ people who are advancing their rights have had their events attacked online and offline (GLAAD 2022) and have faced political persecution (Human Rights Watch 2020). There has been increasing hostility from alt-right groups toward LGBTQ+ people. In Europe, the Office of the Council of Europe Commissioner for Human Rights (2021) found that there was a "sharp increase" against LGBTQ+ human rights defenders and LGBTQ+ people more generally in Europe. As noted earlier in this report, LGBTQ+ activists who defend their rights in certain countries have the violence they face legitimized by society and the state.

96 See Palumbo and Sienra (2017).

97 See Kraicer and Dhrodia (2021).

98 See Abdullah and Campbell (2021).

99 See Sallam (2018).

100 See Vasudevan (2018).

101 Ibid.

102 See Kovacs, Padte and SV (2013).

103 See Iyer, Nyamwire and Nabulega (2020).

104 See Global Information Society Watch (2017).

105 See Lokot (2018).

of those who reported experiencing at least one of the forms of online harm identified social media as the platform where it occurred.

Survey Results: Experiences, Opinions and Impacts

The following sections detail the results of the survey regarding participants' personal experiences with, opinions about and views on the impacts of online harms.

Survey Results: Type of Platform

When asked about their own personal experience with online harms, there were relatively few statistical differences in personal experiences with online harms on various platforms based on participants' gender identity and sexual orientation. As such, the statistics below are inclusive of all participants, regardless of gender identity or sexual orientation.[106]

The most common way people experienced online harms was through social media sites. Seventy-one percent of those who reported experiencing at least one of the forms of online harm identified social media as the platform where it occurred (55 percent reported that it occurred on communication-based social media such as Facebook; 27.8 percent reported that it occurred on image-sharing social media such as Instagram; 20.9 percent reported that it occurred on video-sharing social media such as TikTok; 7.5 percent reported that it occurred on a professional website such as LinkedIn; and 7.0 percent reported that it occurred on a message board such as Reddit).

The next most common method was through direct messages. Sixty-five percent of people who reported having experienced one of the forms of online harm identified direct messages as the platform where it occurred (38.7 percent reported that it occurred on messaging apps such as WhatsApp; 29.7 percent reported that it occurred via email; 29.1 percent reported that it occurred via text message; 9.1 percent reported that it occurred on a video-conferencing app such as Zoom; and 8.8 percent reported that it occurred via cloud storage such as iCloud).

Other technologies included the use of location-tracking technology (11.3 percent); on pornography sites (10.1 percent); and smart home devices (7.6 percent). Some other platform or messaging app not included in the listed options was reported by 6.5 percent.

106 It should be noted that gender identity and sexual orientation were not asked in certain countries for legal and safety reasons (Algeria, Jordan, Saudi Arabia, Tunisia and the UAE).

Survey Results: Commonality and Response to Incidents of Online Harm

The following sections detail the rates of incidents of online harm people experienced, and their various responses.

When interpreting the data on incident reporting, it is important to recognize that the severity and level of harm experienced can vary widely under each of these categories. For example, if someone was repeatedly contacted by someone they did not want to be contacted by, it could be distressing, such as a person not taking the hint that a person does not want to be contacted by them any longer, but not cause the recipient significant harm. However, in contrast, it could be a very serious form of violence, such as an ex-intimate partner relentlessly stalking their ex-partner, sending threats, and causing significant fear with the communication. As such, the incident reporting should be interpreted with this nuance in mind. Further, people may have different reactions to various types of behaviour and different perceptions of their degree of harm.

Because people have such a wide range of reactions to these various types of behaviour, incident reporting alone does not necessarily get to the heart of the actual harms experienced — the harmfulness of the types of online harm must also be considered. The following section details the prevalence of each form of online harm, followed by the actual impact of the TFV and the general perceptions of harmfulness reported. A later section considers participants' reports on aspects of their most serious incidents of online harm, where additional information about the harmfulness of these types of behaviour is discussed, as well as the influence of gender identity, gender expression and sexual orientation.

Survey Results: Experiences with Any Form of Online Harm

Among the survey participants, 59.7 percent had experienced at least one form of online harm. The most common form of online harm experienced by participants was being repeatedly contacted by someone they do not want to be contacted by (37.7 percent), followed by having unwanted sexual images sent to them (28.1 percent); having someone access their devices or social media accounts belonging to them without permission (24.5 percent); being called discriminatory names or derogatory cultural terms (19.8 percent); having lies posted about them online (17.8 percent); being impersonated online (16.5 percent); experiencing harassment because of their gender,

Almost 40% of participants experienced being repeatedly contacted by someone they do not want to be contacted by.

race, sexual orientation, gender expression or other marginalizing factor (16.3 percent); being monitored, tracked or spied on online (14.7 percent); being doxed (14.7 percent); being blackmailed online (12.1 percent); experiencing networked harassment (11.8 percent); being physically threatened (11.7 percent); and having their nude or sexual images shared or shown to someone else or posted online without permission (7.6 percent).

A higher proportion of transgender and gender-diverse people reported experiencing any form of online harm (67.8 percent) than women (59.9 percent) and men (57.0 percent). A higher proportion of LGB+ people reported experiencing any form of online harm (75.8 percent) than heterosexual people (57.2 percent). A higher proportion of LGB+ transgender and gender-diverse individuals reported experiencing any form of online harm (87.7 percent) than LGB+ women (76.7 percent) and LGB+ men (72.6 percent), who reported similar proportions. A higher proportion of heterosexual women reported experiencing online harm (58.6 percent) than heterosexual men (55.7 percent).

The following 13 forms of online harms are listed in order from the most commonly experienced overall to least commonly experienced overall. Where there are statistically significant differences between gender and sexual orientation, they are noted.

Repeated Unwanted Contact

In total, 37.7 percent of participants reported being repeatedly contacted by someone they do not want to be contacted by. A higher proportion of transgender and gender-diverse people (40.3 percent) and women (39.4 percent) reported being repeatedly contacted by someone they do not want to be contacted by than men (31.3 percent). A higher proportion of LGB+ people reported being repeatedly contacted by someone they do not want to be contacted by (46.3 percent) than heterosexual people (34.6 percent).

Unsolicited Sexual Images

Being sent unwanted sexual images was reported by 28.1 percent of participants. The proportion of transgender and gender-diverse people (31.1 percent) and women (28.9 percent) who reported having unwanted sexual images sent to them did not statistically differ; however, a higher proportion of women and transgender and gender-diverse people reported this type of abuse than men (22.8 percent). A higher proportion of LGB+ people reported having unwanted sexual images sent to them (40.1 percent) than heterosexual people (24.8 percent).

Unauthorized Access

Someone accessing their devices or social media accounts without permission was reported by 24.5 percent of all participants. A higher proportion of LGB+ people reported unauthorized access (32.8 percent) than heterosexual people (24.1 percent). There was no statistical difference between genders.

Discrimination

Among all participants, 19.8 percent reported being called discriminatory names or having derogatory cultural terms stated about them. A higher proportion of transgender and gender-diverse people reported being called discriminatory names or having derogatory cultural terms stated about them (30.6 percent) than men (18.8 percent) and women (17.8 percent), who did not statistically differ in their proportions. A higher proportion of LGB+ people reported being called discriminatory names or having derogatory cultural terms stated about them (36.6 percent) than heterosexual people (17.0 percent).

A higher proportion of LGB+ people reported having lies spread about them (29.3 percent) than heterosexual people (17.4 percent).

False Information

Having lies posted about them online was reported by 17.8 percent of all participants. A

higher proportion of transgender and gender-diverse people reported having lies spread about them (30.1 percent) than men (19.8 percent) and women (16.5 percent). A higher proportion of LGB+ people reported having lies spread about them (29.3 percent) than heterosexual people (17.4 percent). A higher proportion of LGB+ transgender and gender-diverse people reported having lies spread about them (41.8 percent) than LGB+ men (25.5 percent) and women (30.9 percent), who reported similar proportions. A higher proportion of heterosexual transgender and gender-diverse people (24.0 percent) and heterosexual men (19.3 percent), who reported similar proportions, reported having lies spread about them than heterosexual women (15.3 percent).

Impersonation

Among survey participants, 16.5 percent reported being impersonated online. Transgender and gender-diverse people (19.5 percent) and men (16.6 percent), who reported similar proportions, were more likely to report being impersonated online than women (14.0 percent). A higher proportion of LGB+ people reported being impersonated online (18.2 percent) than heterosexual people (15.1 percent).

Identity-Based Harassment

Experiencing harassment online because of their gender, race, sexual orientation, disability, gender expression or other marginalizing factors (identity-based harassment) was reported by 16.3 percent of all participants. A higher proportion of transgender and gender-diverse people reported experiencing harassment online because of their gender, race, sexual orientation, disability, gender expression or other marginalizing factors (33.9 percent) than women (15.8 percent) and men (13.3 percent). A higher proportion of LGB+ people reported experiencing harassment online because of their gender, race, sexual orientation, disability, gender expression or other marginalizing factors (36.3 percent) than heterosexual people (13.1 percent).

Monitored, Tracked or Spied On

Being monitored, tracked or spied on online was reported by 14.7 percent of all participants. A higher proportion of transgender and gender-diverse people reported being monitored, tracked or spied on online (24.0 percent) than men (14.6 percent) and women (12.5 percent). A higher proportion of LGB+ people reported being monitored, tracked or spied on online (18.6 percent) than heterosexual people (13.3 percent).

A higher proportion of heterosexual transgender and gender-diverse people (21.3 percent) reported being monitored, tracked or spied on online than heterosexual men (14.5 percent) and heterosexual women (11.9 percent; heterosexual men > women). A higher proportion of LGB+ transgender and gender-diverse people (29.1 percent) reported being monitored, tracked or spied on online than LGB+ men (15.5 percent) but were not different from LGB+ women (19.7 percent). A higher proportion of LGB+ women reported being monitored, tracked or spied on online (19.7 percent) than heterosexual women (11.9 percent).

Doxing

Of all participants, 14.7 percent reported having their personal contact information or their address posted online without permission (doxing). A higher proportion of transgender and gender-diverse people reported being doxed (23.6 percent) than men (17.1 percent) and women (12.8 percent). LGB+ people were just as likely as heterosexual people to report being doxed.

A higher proportion of transgender and gender-diverse people reported being blackmailed online (23.1 percent) than men (12.7 percent) and women (10.1 percent).

Blackmail

Being blackmailed online was reported by 12.1 percent of all participants. A higher proportion of transgender and gender-diverse people reported

being blackmailed online (23.1 percent) than men (12.7 percent) and women (10.1 percent). LGB+ people were more likely to report being blackmailed online (18.6 percent) than those identifying as heterosexual people (11.0 percent).

Networked Harassment

Experiencing networked harassment was reported by 11.8 percent of all participants. A higher proportion of transgender and gender-diverse people reported experiencing networked harassment (27.8 percent) than men (11.5 percent) and women (9.3 percent). A higher proportion of LGB+ people reported experiencing networked harassment (19.6 percent) than heterosexual individuals (9.9 percent). There was an interaction between gender and sexual orientation: the effect of sexual orientation held for women (LGB+ = 19.4 percent; heterosexual = 8.5 percent) and men (LGB+ = 18.1 percent; heterosexual = 11.0 percent), but the proportion of transgender and gender-diverse people reporting networked harassment did not vary by sexual orientation (LGB+ = 29.9 percent; heterosexual = 26.7 percent). A higher proportion of LGB+ transgender and gender-diverse people reported experiencing networked harassment (29.9 percent) than LGB+ women (19.4 percent) and LGB+ men (18.1 percent), who were equally likely to report this type of abuse. A higher proportion of heterosexual transgender and gender-diverse people reported experiencing networked harassment (26.7 percent) than men (11.0 percent) and women (8.5 percent).

Physical Threats

Among participants, 11.7 percent reported being physically threatened. A higher proportion of transgender and gender-diverse people reported being physically threatened (28.1 percent) than men (13.8 percent) and women (11.1 percent). A higher proportion of LGB+ people reported being physically threatened (25.5 percent) than heterosexual people (11.6 percent). A higher proportion of LGB+ transgender and gender-diverse people reported being physically threatened (47.4 percent) than LGB+ women (25.4 percent) and LGB+ men (21.6 percent) who reported similar proportions. A statistically higher proportion of heterosexual transgender and gender-diverse people (18.3 percent) and men (13.1 percent), who reported similar proportions, reported being threatened than women (10.0 percent).

NCDII

Having personal nude or sexual images of them shared or shown to someone else or posted online without permission was reported by 7.6 percent of all participants. A higher proportion of transgender and gender-diverse people reported having personal nude or sexual images of them shared or shown to someone else or posted online without permission (19.2 percent) than men (8.4 percent) and women (6.7 percent). A higher proportion of LGB+ people reported having personal nude or sexual images of them shared or shown to someone else or posted online without permission (16.6 percent) than heterosexual people (7.0 percent).

Survey Results: Reported Impacts of Online Harms

Participants who had experienced at least one form of online harm were asked to rate what impact online harms had on them personally. Because participants reported experiencing multiple forms of online harm, their responses are not separated into individual types of online harm but reflect their general experience.

Participants were asked to rate the impact on their lives on a five-point scale with 5 being “very negatively impacted” and 1 being “no impact at all.” The data discussed below represents those who selected 5, very negatively impacted. As such, the data represents only those who were most seriously impacted and not those who reported lesser impact or no impact.

The following forms of harm are listed in order of most reported as extremely harmful to least.

Table 1: Impacts of Online Harms

	Very negatively impacted 5	4	3	2	No impact at all 1
Mental health	27.7%	18.8%	19.5%	13.5%	20.6%
Personal reputation	**24.7%**	17.5%	17.7%	12.7%	27.5%
Ability to engage freely online	**22.5%**	20.4%	21.1%	12.4%	23.6%
Freedom to express political or personal views	**21.7%**	17.8%	20.1%	12.9%	27.5%
Ability to focus	**20.4%**	18.2%	20.7%	14.6%	26.1%
Close relationships	**20.3%**	17.5%	19.7%	14.2%	28.3%
Physical safety	**19.3%**	17.7%	18.5%	13.5%	31.1%
Employment or business	**18.0%**	16.5%	18.0%	13.1%	34.4%
Desire to live	**16.8%**	13.5%	14.3%	12.0%	43.4%
Sexual autonomy and freedom	**16.2%**	16.0%	17.0%	13.1%	37.7%

Mental Health

The negative impact of online harms was most significant on mental health, with 27.7 percent of all the participants who reported experiencing one of the forms of online harm saying that their mental health was very negatively impacted. A higher proportion of women and transgender and gender-diverse people (similar proportions of 29.4 percent and 29.8 percent, respectively) than men (21.8 percent) reported online harms very negatively impacted their mental health. A higher proportion of LGB+ people reported that online harms very negatively impacted their mental health (35.8 percent) than heterosexual people (24.7 percent).

Personal Reputation

Nearly one-quarter of all participants who experienced one of the forms of online harm identified (24.7 percent), reported a very negative impact on their personal reputation; however, there was no significant difference in the negative impact of online harms on personal reputation based on sexual orientation or gender.

Ability to Engage Freely Online

Among all participants who reported experiencing one of the forms of online harm identified, 22.5 percent said it had a very negative impact on their ability to engage freely online. A higher proportion of women than men reported a very negative impact on their ability to engage freely online (22.9 percent compared to 18.6 percent). There was no statistically significant difference between transgender and gender-diverse people (20.1 percent) and women or men. There was also no statistically significant difference between heterosexual and LGB+ people.

Freedom to Express Political or Personal Views

Of all the participants who reported experiencing one of the forms of online harm identified, 21.7 percent said that online harms very negatively

impacted their freedom to express their political and personal views. A higher proportion of LGB+ people reported online harms very negatively impacted their freedom to express their political and personal views (25.5 percent) than heterosexual people (19.5 percent). There was no significant difference between genders.

A higher proportion of LGB+ people reported that online harms very negatively impacted their mental health (35.8 percent) than heterosexual people (24.7 percent).

Ability to Focus

Of those participants who had experienced one of the forms of online harm identified, 20.4 percent reported a very negative impact on their ability to focus. A higher proportion of transgender and gender-diverse people reported a very negative impact on their ability to focus (26.4 percent) than women (19.8 percent) and men (16.3 percent). A higher proportion of LGB+ people reported a very negative impact on their ability to focus (22.9 percent) than heterosexual people (17.8 percent).

Close Relationships

Of all the participants who had experienced one of the forms of online harm, 20.3 percent reported a very negative impact on their close relationships. A higher proportion of LGB+ people reported a very negative impact on their close relationships (22.0 percent) than heterosexual people (17.7 percent). There was no significant difference between genders.

Physical Safety

Among participants who had experienced one of the forms of online harm identified, 19.3 percent reported that online harms very negatively impacted their personal safety. A higher proportion of transgender and gender-diverse people (24.4 percent) and women (20.7 percent) reported that online harms very negatively impacted their personal safety compared to men (16.3 percent). A higher proportion of LGB+ people reported that online harms very negatively impacted their personal safety (24.2 percent) than heterosexual people (17.9 percent). A higher proportion of LGB+ women reported that online harms very negatively impacted their personal safety (27.8 percent) than heterosexual women (19.8 percent). A higher proportion of LGB+ men reported that online harms very negatively impacted their personal safety (22.0 percent) than heterosexual men (15.5 percent). A higher proportion of heterosexual transgender and gender-diverse people reported that online harms very negatively impacted their personal safety (28.9 percent) than heterosexual women (19.8 percent) and men (15.5 percent). LGB+ people of all genders reported similar proportions.

Employment or Business

Eighteen percent of all the participants who reported experiencing one of the forms of online harm identified stated that online harms very negatively impacted their employment or business. Transgender and gender-diverse people were most likely to report that online harms very negatively impacted their employment or business (28.8 percent). The proportion for men and women was similar — 17.5 percent and 15.9 percent, respectively. There was no significant difference between heterosexual and LGB+ people.

Desire to Live

Among all the participants, 16.8 percent of those who reported experiencing one of the forms of online harm said it very negatively impacted their desire to live. A higher proportion of transgender and gender-diverse people reported that online harms very negatively impacted their desire to live (29.6 percent) compared to women (15.8 percent) and men (13.6 percent). A higher proportion of LGB+ people reported that online harms very negatively

impacted their desire to live (22.9 percent) than heterosexual people (14.1 percent).

Sexual Autonomy and Freedom

Among participants who reported experiencing one of the forms of online harm identified, 16.2 percent stated that online harms very negatively impacted their sexual autonomy and freedom. A higher proportion of transgender and gender-diverse people reported it very negatively impacted their sexual autonomy and freedom (28.4 percent) than women (16.8 percent) and men (14.6 percent). A higher proportion of LGB+ people reported online harms very negatively impacted their sexual autonomy and freedom (25.1 percent) than heterosexual people (14.9 percent). A higher proportion of LGB+ women reported online harms very negatively impacted their sexual autonomy and freedom (21.5 percent) than heterosexual women (16.4 percent). A higher proportion of LGB+ men (26.9 percent) reported online harms very negatively impacted their sexual autonomy and freedom than heterosexual men (13.0 percent). A statistically similar proportion of LGB+ transgender and gender-diverse people reported online harms very negatively impacted their sexual autonomy and freedom (35.4 percent) than heterosexual transgender and gender-diverse people (23.8 percent). A statistically higher proportion of heterosexual transgender and gender-diverse people (23.8 percent) and heterosexual women (16.4 percent), who reported similar proportions, reported that online harms very negatively impacted their sexual autonomy compared to heterosexual men (13.0 percent).

Survey Results: Actions Taken

Respondents who had experienced some form of online harm were asked what actions they took in response. There were relatively little statistically significant differences between the gender and sexual orientation of individuals and the actions they took in response to online harms. As such, the statistics below are inclusive of all participants of the survey, regardless of gender or sexual orientation.[107]

In response to an incident of online harm, higher proportions of people blocked or muted someone (51.7 percent), changed their privacy settings (37.6 percent), took a break from social media (26.7 percent), or deleted or deactivated their social media account (25.2 percent).

The next most common responses included people who reported that they changed their contact information (24.2 percent), stopped or reduced posting on a certain platform (23.2 percent), stopped posting about a certain issue (19.8 percent), changed their profile information (18.6 percent), searched for content about themselves online (15.5 percent), or changed their behaviour in a relationship (14.5 percent).

Lower proportions of people acted differently to protect their safety: respondents reported they changed the route they normally walk (14.4 percent); avoided social occasions or events (13.9 percent); replaced their devices with a new one (11.3 percent); stopped participating online altogether (10.8 percent); changed part of their identity, such as how they look or their legal name (8.0 percent); bought something to add to their security (7.1 percent); took time off school or work (6.8 percent); or moved to another address (5.9 percent).

"None of the above" was the response given by 10.5 percent of respondents.

Survey Results: Perceptions of Harmfulness of Online Harms

The survey also asked people about their general perceptions of how big a problem OGBV was for various groups of people in their country. They were also asked about each of the 13 different forms of online harms and asked to rate how harmful they thought they were. All participants — those who had experienced online harms and those who had not — were asked this question.

107 It should be noted that data on gender identity and sexual orientation was not collected in all countries.

Close to  **of participants reported that OGBV was a very big problem for LGBTQ+ people.**

Survey Results: Perceptions of Who OGBV Is a Big Problem For

Participants were asked how big of an issue OGBV is for "women in your country," "men in your country," "transgender/non-binary individuals/ non-heterosexual individuals (e.g., lesbian/gay/ bisexual) in your country" and "yourself" on a five-point scale with 5 as a "very big problem" and 1 as "not a problem at all." Participants recognized that OGBV was a bigger problem for LGBTQ+ people and women than men. Participants reported that it was a very big problem for LGBTQ+ people (46.5 percent) and women (44.3 percent) compared to men (22.7 percent). When asked about OGBV, 28.4 percent of all participants identified that it was a very big problem for themselves. A higher proportion of women (25.9 percent) than men (21.7 percent) reported OGBV as being a very big problem for themselves.

Close to half, 46.5 percent, reported that OGBV was a very big problem for LGBTQ+ people (higher proportion of women, 51.4 percent, than men, 42.4 percent, and transgender and gender-diverse individuals, 41.6 percent). Among all participants, 44.3 percent reported that OGBV was a very big problem for women (higher proportion of women, 47.7 percent, than men, 38.1 percent, and transgender and gender-diverse individuals, 38.1 percent). And 22.7 percent of participants reported that OGBV was a very big problem for men (higher proportion of women, 22.3 percent, than men, 18.2 percent).[108]

Survey Results: General Perceptions of the Harmfulness of Online Harms

The following section describes the general perceived perceptions of the harmfulness of online harms. Participants were asked to rate how harmful each of the 13 types of online harm would be if it happened to them or someone they knew. All participants were asked to rate each form of online harms on a five-point scale with 5 as "extremely harmful" and 1 as "not very harmful." The following statistics reflect those that selected "extremely harmful." As such, those that rated it as moderately harmful or not very harmful are not included in these numbers. The 13 forms of online harm are listed in order from the type of online harm that was rated by participants as most harmful to the type that was rated as least harmful.

When rating the harmfulness of each of the types of online harm, 76.6 percent of all participants rated NCDII as extremely harmful, followed by physical threats (74.4 percent), blackmail (73.5 percent), impersonation (69.5 percent), networked harassment (68.1 percent), unauthorized access to their devices or accounts (68.0 percent), being monitored, tracked or spied on (66.9 percent), doxing (65.4 percent), having lies posted about them (65.0 percent), receiving unsolicited sexual images (65.0 percent), identity-based harassment (64.6 percent), being called discriminatory or

108 The percentages of gender in the brackets are lower than the total number because some people did not select their gender identity in the survey as there was an option of "Prefer not to answer" and others were not asked based on survey limitations in specific countries.

Table 2: Perceptions of the Harmfulness of Online Harms

	Extremely harmful 5	4	3	2	Not very harmful 1
NCDII	**76.6%**	**11.2%**	**6.2%**	**2.6%**	**3.5%**
Physical threats	**74.4%**	11.9%	6.9%	2.7%	4.1%
Blackmail	**73.5%**	12.5%	6.6%	3.2%	4.3%
Impersonation	**69.5%**	15.9%	8.0%	3.2%	3.4%
Networked harassment	**68.1%**	16.1%	8.3%	3.5%	3.9%
Unauthorized access	**68.0%**	16.7%	8.3%	3.3%	3.7%
Monitored, tracked or spied on	**66.9%**	16.6%	8.9%	3.7%	4.0%
Doxing	**65.4%**	18.1%	9.1%	3.3%	4.0%
Untrue information	**65.0 %**	19.3%	8.8%	3.1%	3.8%
Unsolicited sexual images	**65.0%**	16.6%	10.1%	3.8%	4.4%
Identity-based harassment	**64.6%**	17.8%	9.2%	3.9%	4.5%
Discrimination	**60.5%**	20.1%	10.7%	4.2%	4.4%
Repeated unwanted contact	**49.9%**	24.8%	14.6%	5.4%	5.2%

derogatory cultural terms (60.5 percent) and being repeatedly contacted by someone they did not want to be contacted by (49.9 percent). Women were more likely to report any form of online harms as more harmful than men, and transgender and gender-diverse people.

NCDII

More than three-quarters (76.6 percent) of all participants reported having their nude or sexual images shared or posted without permission as extremely harmful. A higher proportion of women reported having their nude or sexual images shared or posted without permission as extremely harmful (82.8 percent) than men (71.2 percent) and transgender and gender-diverse people (60.0 percent). There was no significant difference between LGB+ people and heterosexual people.

Physical Threats

Physical threats such as death threats, rape threats or threats of physical harm via digital means were considered extremely harmful by 74.4 percent of all participants. A higher proportion of women (80.5 percent) reported threats as extremely harmful than men (68.0 percent) and transgender and gender-diverse people (56.1 percent; women > men > transgender and gender-diverse people). A higher proportion of heterosexual women reported threats as extremely harmful (81.4 percent) than LGB+ women (73.0 percent). A similar proportion of LGB+ men reported threats as extremely harmful (70.4 percent) as heterosexual men (68.1 percent). A higher proportion of heterosexual women (81.4 percent) and heterosexual men (68.1 percent) reported threats as extremely harmful than heterosexual transgender and gender-diverse

people (59.2 percent). A similar proportion of LGB+ women (73.0 percent) and LGB+ men (70.4 percent) reported threats as extremely harmful, which was a higher proportion than LGB+ transgender and gender-diverse people (52.5 percent). A statistically similar proportion of heterosexual transgender and gender-diverse people reported threats as extremely harmful (59.2 percent) than LGB+ transgender and gender-diverse people (52.5 percent). Finally, a higher proportion of heterosexual people reported threats as extremely harmful (74.7 percent) than LGB+ people (70.2 percent).

Blackmail

Being blackmailed online was perceived as extremely harmful by 73.5 percent of all participants. A higher proportion of women reported being blackmailed as extremely harmful (77.8 percent) than men (67.4 percent) and transgender and gender-diverse people (58.3 percent; women > men > transgender and gender-diverse people). A higher proportion of heterosexual women reported being blackmailed as extremely harmful (78.5 percent) than LGB+ women (71.4 percent). A similar proportion of LGB+ men reported being blackmailed as extremely harmful (70.0 percent) as heterosexual men (67.4 percent). A similar proportion of LGB+ transgender and gender-diverse people (61.0 percent) and heterosexual transgender and gender-diverse people (58.3 percent) reported being blackmailed as extremely harmful. A similar proportion of heterosexual people (72.9 percent) and LGB+ people (69.8 percent) reported being blackmailed as extremely harmful. A higher proportion of heterosexual women reported being blackmailed online as extremely harmful (78.5 percent) than heterosexual men (67.4 percent) and heterosexual transgender and gender-diverse people (58.3 percent). A similar proportion of LGB+ women reported being blackmailed online as extremely harmful (71.4 percent) as LGB+ men (70.4 percent) and LGB+ transgender and gender-diverse people (61.0 percent).

Impersonation

Among all participants, 69.5 percent reported being impersonated online as extremely harmful. A higher proportion of women reported being impersonated online as extremely harmful (72.5 percent) than men (65.8 percent) and transgender and gender-diverse people (55.6 percent; women > men > transgender and gender-diverse people). A higher proportion of heterosexual women reported being impersonated online as extremely harmful (73.6 percent) than LGB+ women (61.2 percent). A similar proportion of LGB+ men reported being impersonated online as extremely harmful (65.6 percent) as heterosexual men (66.1 percent). A similar proportion of LGB+ transgender and gender-diverse people reported being impersonated online as extremely harmful (57.0 percent) as heterosexual transgender and gender-diverse people (55.8 percent). A higher proportion of heterosexual people reported being impersonated online as extremely harmful (69.7 percent) than LGB+ people (62.8 percent). A higher proportion of heterosexual women reported being impersonated online as extremely harmful (73.6 percent) than heterosexual men (66.1 percent) and heterosexual transgender and gender-diverse people (55.8 percent).

Networked Harassment

Networked harassment was rated as extremely harmful by 68.1 percent of all participants. Women were more likely to report networked harassment as extremely harmful (74.0 percent) than men (62.0 percent) and transgender and gender-diverse people (58.3 percent), who reported statistically similar proportions. There was no significant difference between LGB+ and heterosexual people.

Unauthorized Access

Sixty-eight percent of all participants perceived unauthorized access to their devices or social media accounts as extremely harmful. A higher proportion of women reported that unauthorized access to their devices or social media accounts was extremely harmful (70.5 percent), than men (62.5 percent) and transgender and gender-diverse people (52.3 percent; women > men > transgender and gender-diverse people). A higher proportion of heterosexual women reported that unauthorized access to their devices or social media accounts was extremely harmful (71.3 percent) than LGB+ women (60.0 percent). A similar proportion of LGB+ men reported that unauthorized access to their devices or social media accounts was extremely harmful (66.5 percent) as heterosexual men (62.4 percent). A statistically similar proportion of LGB+ transgender and gender-diverse people reported that unauthorized access to their devices or social media accounts was extremely harmful (59.5 percent) as heterosexual transgender and gender-diverse

people (50.7 percent). A higher proportion of heterosexual women (71.3 percent) reported that unauthorized access to their devices or social media was extremely harmful than heterosexual men (62.4 percent) and heterosexual transgender and gender-diverse heterosexual people (50.7 percent). A statistically similar proportion of LGB+ women (60.0 percent) perceived unauthorized access to their devices or social media as extremely harmful as LGB+ men (66.5 percent) and LGB+ transgender and gender-diverse people (59.5 percent). A similar proportion of heterosexual people (66.8 percent) and LGB+ people (63.1 percent) reported that unauthorized access to their devices or social media accounts was extremely harmful.

Monitored, Tracked or Spied On

Among all participants, 66.9 percent considered being monitored, tracked or spied on online extremely harmful. A higher proportion of women reported being monitored, tracked or spied on online as extremely harmful (71.5 percent) than men (60.6 percent) and transgender and gender-diverse people (53.6 percent; women > men > transgender and gender-diverse people). A higher proportion of heterosexual women reported being monitored, tracked or spied on online as extremely harmful (72.4 percent) than LGB+ women (65.6 percent). A similar proportion of LGB+ men reported being monitored, tracked or spied on online as extremely harmful (63.2 percent) as heterosexual men (60.6 percent). A statistically similar proportion of LGB+ transgender and gender-diverse people reported being monitored, tracked or spied on online as extremely harmful (58.5 percent) as heterosexual transgender and gender-diverse people (52.1 percent). A similar proportion of heterosexual people (66.5 percent) as LGB+ people (63.9 percent) reported being monitored, tracked or spied on online as extremely harmful. A higher proportion of heterosexual women reported being monitored, tracked or spied on online as extremely harmful (72.4 percent) than heterosexual men (60.6 percent) and heterosexual transgender and gender-diverse people (52.1 percent). Statistically similar proportions of LGB+ women reported being monitored, tracked or spied on online as extremely harmful (65.6 percent) as LGB+ men (63.2 percent), and LGB+ transgender and gender-diverse people (58.5 percent) reported being monitored, tracked or spied on online as extremely harmful.

Doxing

Having their personal contact information or their address posted online without permission (doxing) was perceived as extremely harmful by 65.4 percent of all participants. A higher proportion of women reported doxing as extremely harmful (70.2 percent) than men (59.9 percent) and transgender and gender-diverse people (53.6 percent), whose proportions were statistically similar. A similar proportion of heterosexual women and LGB+ women reported doxing as extremely harmful. A higher proportion of LGB+ men reported doxing as extremely harmful (65.3 percent) than heterosexual men (59.8 percent). A higher proportion of heterosexual women (70.4 percent) reported doxing as extremely harmful than heterosexual men (59.8 percent) and heterosexual transgender and gender-diverse people (51.7 percent), who reported similar proportions. No difference was found in the proportions of LGB+ transgender and gender-diverse people and heterosexual transgender and gender-diverse people who reported doxing as extremely harmful. Similar proportions of LGB+ women, men and transgender and gender-diverse people reported doxing as extremely harmful. Similar proportions of heterosexual people and LGB+ people reported that doxing was extremely harmful.

Untrue Information

Sixty-five percent of all participants reported having lies posted about them online as extremely harmful. Women were more likely to report having lies posted about them online as extremely harmful (67.9 percent) than men (59.3 percent) and transgender and gender-diverse people (53.0 percent). A higher proportion of heterosexual women reported having lies posted about them online was extremely harmful (68.5 percent) than LGB+ women (58.3 percent). A similar proportion of LGB+ men reported that having lies posted about them online was extremely harmful (60.2 percent) as heterosexual men (59.2 percent). A statistically similar proportion of heterosexual transgender and gender-diverse people reported that having lies posted about them online was extremely harmful (57.2 percent) as LGB+ transgender and gender-diverse people (48.7 percent). A higher proportion of heterosexual people reported that having lies posted about them online was extremely harmful (64.0 percent) than LGB+ people (58.3 percent). A higher proportion of heterosexual women reported

having lies posted about them online was harmful (68.5 percent) than heterosexual men (59.2 percent) and heterosexual transgender and gender-diverse people (57.2 percent), who reported a similar proportion.

Unsolicited Sexual Images

The same proportion (65.0 percent) of all participants reported unwanted sexual images sent to them as extremely harmful. A higher proportion of women reported that receiving unsolicited sexual images was extremely harmful (70.4 percent) than men (54.9 percent) and transgender and gender-diverse people (53.2 percent; women > men > transgender and gender-diverse people). A higher proportion of heterosexual people reported that receiving unsolicited sexual images was extremely harmful (63.5 percent) than LGB+ people (54.6 percent).

Identity-Based Harassment

Of all participants, 64.6 percent reported experiencing harassment online because of their gender, race, sexual orientation, disability, gender expression or other marginalizing factors as extremely harmful. Women were more likely to report that identity-based harassment was extremely harmful (68.4 percent) than men (55.4 percent) and transgender and gender-diverse people (48.9 percent; women > men > transgender and gender-diverse people). There was no significant difference between LGB+ and heterosexual people.

Discrimination

Of all participants, 60.5 percent reported being called discriminatory or derogatory names online as extremely harmful. A higher proportion of women reported being called discriminatory or derogatory names online as extremely harmful (64.9 percent) than men (51.2 percent) and transgender and gender-diverse people (48.1 percent), whose proportions were similar. There was no significant difference between LGB+ people and heterosexual people.

Repeated Unwanted Contact

Half of all participants (49.9 percent) reported repeated unwanted contact as extremely harmful. Women were more likely to report repeated unwanted contact as extremely harmful (55.6 percent) than transgender and gender-diverse people (43.8 percent), and men (43.4 percent), who reported similar proportions. More heterosexual women reported repeated unwanted contact as extremely harmful (56.5 percent) than LGB+ women (46.2 percent). Similar numbers of LGB+ men reported repeated unwanted contact as extremely harmful (42.2 percent) as heterosexual men (43.6 percent). A statistically similar proportion of heterosexual transgender and gender-diverse people reported repeated unwanted contact as extremely harmful (49.0 percent) as LGB+ transgender and gender-diverse people (39.7 percent). Heterosexual people were more likely to report repeated unwanted contact as extremely harmful (50.2 percent) than LGB+ people (43.8 percent).

Survey Results: Young People (Aged 25 and Under)

Close to one-quarter of participants (23.7 percent) were young people (aged 25 years and under; 16–25 years) and 76.3 percent were older adults (over the age of 25; 26–74 years). A higher proportion of young people aged 25 and under reported having personally experienced at least one type of harm listed (68.5 percent) than people over the age of 25 (56.9 percent), and reported the attack had a very negative impact on their personal life (in all categories other than employment, freedom to express political or personal views, and personal reputation, where there was no difference in the two age categories). A higher proportion of young people reported they had been targeted because of identity factors, including gender identity (27.5 percent versus 23.4 percent), gender expression (10.2 percent versus 7.5 percent), age (17.9 percent versus 11.8 percent) and sexual orientation (8.8 percent versus 6.4 percent), than older people. Similar proportions of younger and older people reported being targeted due to race/ethnicity, religion and disability. A lower proportion of young people rated each individual behaviour as harmful than older adults (in all categories other than non-consensual image sharing, receiving unsolicited sexual images and identity-based harassment, where there was no difference in the two age categories).

Survey Results: High-Profile People

Among all respondents, 12.4 percent can be considered high-profile people (identified as advocate/activist, journalist, social media influencer or politician). A higher proportion of high-profile people (77.2 percent) had personally experienced at least one form of online harm than non-high-profile people (57.2 percent). They were more likely to experience reputation and identity-based harms (60.3 percent versus 34.3 percent),[109] coercion and harassment (64.4 percent versus 42.2 percent),[110] privacy and security-based harms (54.6 percent versus 31.5 percent),[111] and sexual harms (45.3 percent versus 27.1 percent)[112] than those who would not be considered high-profile people.

Survey Results: Most Serious Incident

Of those participants who had experienced at least one form of online harm, participants were asked to consider the most serious incident that they experienced. As many harms intersect in online attacks (for example, nude photos of someone posted along with derogatory comments, threats and their address, combining several forms of online harm) participants were only asked a generalized question about the most serious incident they experienced.

Frequency of Incident(s)

Of the most serious incidents that people experienced, it was most likely to be a one-off incident (43.1 percent) or to have occurred a few times (44.2 percent). Chronic attacks that occurred monthly, weekly and daily were less common (12.6 percent).

In their most serious incidents, a higher proportion of transgender and gender-diverse people experienced chronic attacks (25.5 percent) than men (14.3 percent) and women (13.7 percent). A higher proportion of LGB+ people experienced chronic attacks (19.3 percent) than heterosexual people (13.5 percent). Chronic attacks included all events that happened monthly, weekly or daily.

Reason for Being Targeted

Gender Identity

Of those who reported on their gender identity, 50.4 percent identified as women, 47.5 percent identified as men and 2.0 percent identified as transgender and/or gender diverse.

When considering the most serious incident of online harm they had experienced, 24.5 percent of all participants identified that their gender identity was the reason they were targeted. A higher proportion of transgender and gender-diverse people (31.8 percent) and women (29.8 percent), who reported similar proportions, reported their gender identity as the reason they were targeted than men (16.0 percent). A higher proportion of LGB+ people (28.7 percent) reported their gender identity as the reason they were targeted than heterosexual people (23.0 percent).

Gender Expression

When considering the most serious incident of online harm they had experienced, 8.3 percent of all participants identified that their gender expression was the reason they were targeted. A higher proportion of transgender and gender-diverse people (24.0 percent) reported their gender expression as the reason they were targeted than men (8.6 percent) and women (8.2 percent), who reported similar proportions. A higher proportion of LGB+ people (17.8 percent) report their gender expression as the reason they were targeted than heterosexual people (7.8 percent).

Race/Ethnicity

When considering the most serious incident of online harm they had experienced, 14.5 percent of all participants identified that their race/ethnicity was the reason they were targeted. A higher proportion of men (17.6 percent) and transgender and gender-diverse people (17.0 percent), who

109 Identity and reputation-based harms included online impersonation, lies posted about them online, identity-based harassment and called discriminatory names.

110 Coercion and harassment included threats, blackmail, networked harassment and repeated unwanted contact.

111 Privacy and security-based harms included someone accessing someone else's device without permission, tracking/monitoring and doxing.

112 Sexual harms included sexual images shared without consent and unsolicited sexual images.

reported similar proportions, reported their race/ethnicity as the reason they were targeted than women (9.7 percent).

The original survey included a category for participants to identify their race and ethnicity. However, racial and ethnic data was not collected in most countries by those collecting the data for this report.[113] The authors of this report were not made aware of this until after the data collection was complete and, as such, were unable to provide international statistics on racial or ethnic minorities impacted by online harms.

Age

When considering the most serious incident of online harm they had experienced, 13.5 percent of all participants identified that their age was the reason they were targeted. There were no significant differences by sexual orientation or gender. Almost one-quarter of participants were under the age of 25 (23.7 percent); 69.4 percent were between the ages of 24 and 64; and 6.9 percent were over the age of 65.

Sexual Orientation

Of those participants who were asked about their sexual orientation and reported it, 92.0 percent identified as heterosexual, and 8.0 percent identified as LGB+.[114]

When considering the most serious incident of online harm they had experienced, 7.0 percent of all participants identified that their sexual orientation was the reason they were targeted (8.0 percent of participants who reported their sexual orientation identified as LGB+). A higher proportion of transgender and gender-diverse people (25.7 percent) reported their sexual orientation as the reason they were targeted than men (12.2 percent) and women (7.9 percent). A higher proportion of LGB+ people (42.7 percent) reported their sexual orientation as the reason they were targeted than heterosexual people (6.6 percent). This was true across gender: 53.3 percent of LGB+ men compared to 7.8 percent of heterosexual men; 42.3 percent of LGB+ transgender and gender-diverse people compared to 11.3 percent of heterosexual transgender and gender-diverse people; and 32.6 percent of LGB+ women compared to 5.4 percent of heterosexual women. A higher proportion of heterosexual transgender and gender-diverse people (11.2 percent) and heterosexual men (7.8 percent) reported their sexual orientation as the reason they were targeted than heterosexual women (5.4 percent).

A higher proportion of LGB+ people (42.7 percent) reported their sexual orientation as the reason they were targeted than heterosexual people (6.6 percent).

Religion

When considering the most serious incident of online harm they had experienced, 12.1 percent of participants identified that their religion was the reason they were targeted. Higher proportions of transgender and gender-diverse people (14.1 percent) and men (13.9 percent), who reported similar proportions, reported their religion as the reason they were targeted than women (7.7 percent). There were no significant differences by sexual orientation.

113 Data on race and ethnicity was only collected in Canada, Jordan, Saudi Arabia, the UAE and the United States. Ipsos, which conducted the data collection, provided the following statement: "For the race/ethnicity, as mentioned before, for the purposes of development of the demographic questions for each country, standard Ipsos demographic questions used in global studies were referenced as a starting point, and further adaptations were made based on the needs of this survey. At the time of survey development (2020), it was not common to ask race/ethnicity questions in many countries. Therefore, based on the advice of the in-country experts, race/ethnicity questions were only asked in countries where it was not considered sensitive and/or offensive. Over the last year, growing awareness and focus on Diversity, Equity and Inclusion initiatives have meant that the collection of race and ethnicity information has become more common and acceptable than it was a few years ago. As a result, this information can be collected in many more countries than it was acceptable when the survey was developed and fielded (2020–2021)."

114 For safety reasons, participants in Algeria, Jordan, Saudi Arabia, Tunisia and the UAE were not asked about their sexual orientation.

Table 3: Religious Affiliation

Religion	Proportion of Participants
Sunni Muslim	24.5%
Catholic	24.4%
Protestant or Evangelical	10.3%
Atheist	9.4%
Hindu	5.5%
Another form of Christian	5.4%
Spiritual but not religious	5.3%
Agnostic	4.3%
Buddhist	1.6%
Another religion	1.0%
Christian Orthodox	0.9%
Another form of Muslim	0.9%
Jehovah's Witness	0.7%
Shi'a Muslim	0.7%
Jewish	0.5%
Confucianism	0.4%
Sikh	0.2%
Mormon	0.2%
Prefer not to answer	3.9%

Disability

When considering the most serious incident of online harm they had experienced, 3.5 percent of all participants identified that their disability was the reason they were targeted (11.0 percent of individuals identified as having a disability). Higher proportions of transgender and gender-diverse people (7.0 percent) and men (5.4 percent), who reported similar proportions, reported their disability as the reason they were targeted than women (2.7 percent). There were no significant differences by sexual orientation.

No Identity Factor

For 37.4 percent of participants, none of the identity factors listed were the reason they thought they were targeted.

Person Causing the Harm

Considering the most serious incident of online harm they had experienced, most people (64.1 percent) reported that the person who targeted them was unknown to them or a distant but identifiable person, where the person was someone they had never met (32.1 percent), an anonymous person (27.2 percent), the person's identity couldn't be determined (11.1 percent), a random group of people (9.6 percent), was a member of an identifiable online group (7.0 percent), or was a politician or public authority figure (2.8 percent).

The next most common group was a close relationship (31.5 percent), such as a friend (14.7 percent), ex-intimate partner (12.8 percent), family member (6.4 percent) or current intimate partner (4.3 percent).

The next most common group was people who are known to the person (21.3 percent), but not a close relationship, such as a co-worker (9.0 percent), another student (8.9 percent), a client/customer (4.7 percent) or a teacher (3.1 percent).

Among participants, 4.5 percent said it was another person not listed.

Gender of Person Causing the Harm

Do Not Know the Gender

Of the most serious incidents of online harm reported, 24.8 percent reported that they did not know the gender of the person who targeted them.

Men

Men were, by far, the most common gender of person instigating the most serious incidents of online harm. Of the most serious incidents of online harm reported, 49.7 percent reported that it was a man who targeted them, the highest percentage of all gender categories. Specifically, 57.7 percent of women, 51.6 percent of transgender and gender-

diverse people and 42.9 percent of men reported that it was a man who targeted them.

Women

Of the most serious incidents of online harm reported, 18.9 percent reported that it was a woman who targeted them. Specifically, 23.1 percent of men, 25.8 percent of transgender and gender-diverse people and 18.1 percent of women reported that a woman attacked them.

Other Gender

Of the most serious incidents of online harm reported, 1.1 percent reported that it was a person of a gender other than man or woman who targeted them.[115]

Summary of Survey Results: Personal Experiences with Online Harms in Relation to Gender and Sexual Orientation

TFV is a widespread problem internationally. These data show that most people surveyed reported that they had experienced at least one form of online harms (59.7 percent).

The data revealed several interesting trends that demonstrated the influence of gender, gender identity and sexual orientation on online harms, which will be discussed below.

Transgender and Gender-Diverse People

When reporting incidents of online harm, transgender and gender-diverse people experienced higher overall proportions of incidents than the general participants: 67.8 percent reported experiencing at least one form of online harm compared to 59.7 percent of the overall participants. They also reported higher proportions of incidents in most individual categories of online harm.

Transgender and gender-diverse people were particularly vulnerable to networked harassment (27.8 percent); having their intimate images shared without consent (19.2 percent); being threatened (28.1 percent); being called discriminatory names or having derogatory cultural terms stated about them (30.6 percent); as well as being targeted because of their gender, race, sexual orientation, disability, gender expression or other marginalizing factor (33.9 percent). They reported close to double the amounts of these types of harms compared to men and women in several categories.

The increased visibility and hostility toward transgender and gender-diverse people has been reported in previous research, and the survey data reflects the heightened experiences of discrimination that these groups face in the digital and physical world (GLAAD 2022). They were also much more likely to be monitored, tracked or spied on (24.0 percent), doxed (23.6 percent), blackmailed (23.1 percent) or to have untrue information posted about them online (30.1 percent). This pattern matches up with previous research that shows that some individuals and groups online are actively seeking to bring negative attention to members of the LGBTQ+ population that can put them at risk of online and offline harms (Curlew and Monaghan 2019). This data demonstrates the need for supports and education to be specifically aimed at preventing online harms against LGBTQ+ people as they are proportionately the most targeted group.

Transgender and gender-diverse people were particularly vulnerable to networked harassment, having their intimate images shared without consent and being threatened.

115 For legal and safety reasons, participants in Algeria, Jordan, Saudi Arabia, Tunisia and the UAE were not asked about gender identity.

In terms of the actual impact of online harms on transgender and gender-diverse people, they faced some of the most negative impacts to their mental health (29.8 percent), ability to focus (26.4 percent), physical safety (24.4 percent), desire to live (29.6 percent), employment and business (28.8 percent) and sexual autonomy (28.4 percent), compared to the other gender categories. The impact on their desire to live is particularly concerning because rates of suicide among transgender and gender-diverse people are much higher than the average population (Virupaksha, Muralidhar and Ramakrishna 2016; Bauer et al. 2013), and this data shows that online harms can affect their desire to live. The increased risks to physical safety are equally concerning. Transgender and gender-diverse people face disproportionately high rates of physical attacks (Ghoshal 2020), and online harms contribute to their already precarious sense of safety in the world. The data on employment and business is relevant as well: many transgender people face barriers in securing employment because of discrimination against them (Trans PULSE 2011; Hébert et al. 2022). Online harms may include doxing or shaming transgender people online in ways that impact their ability to maintain employment and live freely and safely. Discrimination against transgender people is also associated with their ability to find sexual and romantic partners and live with sexual autonomy (Scheim and Bauer 2019; Ashley 2018b). These challenges were reflected in the data, which showed a higher proportion of transgender people's sexual autonomy being impacted by online harms.

When considering the most serious incident of online harm experienced, transgender and gender-diverse people were the most likely to experience chronic attacks that occurred monthly, weekly or daily (25.5 percent). This trend has been shown in previous research describing organized disinformation campaigns and organized harassment of transgender and gender-diverse individuals (Curlew and Monaghan 2019). These relentless forms of online attacks disrupt the lives of transgender and gender-diverse people, who deserve to be able to exist authentically and safely in digital spaces.

Transgender and gender-diverse people were most likely to report being targeted because of their gender identity (31.8 percent), gender expression (24.0 percent), religion (14.1 percent) or disability (7.0 percent), and were among the most likely groups to report being targeted due to their race or ethnicity (17.0 percent) or sexual orientation (25.7 percent). In nearly all identity factors, it was shown that transgender and gender-diverse people are discriminatorily targeted against, negatively affecting their human rights.

Transgender and gender-diverse people were the most likely to experience chronic attacks that occurred monthly, weekly or daily (25.5 percent).

These relentless forms of online attacks disrupt the lives of transgender and gender-diverse people, who deserve to be able to exist authentically and safely in digital spaces.

LGB+ People

LGB+ people also reported a higher proportion of incidents of online harm (75.8 percent) compared to heterosexual people (57.2 percent). LGB+ people also reported higher rates of online harm in many categories, including threats (25.5 percent); unwanted contact (46.3 percent); blackmail (18.6 percent); unauthorized access to their devices and accounts (32.8 percent); being called discriminatory names or having derogatory cultural terms stated about them (36.6 percent); untrue information being posted about them (29.3 percent); harassed online because of their gender, race, sexual orientation, disability, gender expression or other marginalizing factors (36.3 percent); and monitored, tracked or spied on online (18.6 percent). Like transgender and gender-diverse people, LGB+ people continue to be discriminated against globally (eSafety Commissioner 2021), including through disinformation campaigns online (Strand and Svensson 2021).

More than

% of LGB+ people reported that online harms very negatively impacted their mental health.

This data shows that online harm is a contributing factor to the inequality LGB+ people face on a regular basis.

LGB+ people reported some of the most negative effects on their mental health (35.8 percent), their freedom to express political or personal views (25.5 percent), their ability to focus (22.9 percent), their close relationships (22 percent), their physical safety (24.2 percent), their desire to live (22.9 percent) and their sexual autonomy (25.1 percent). The high rates of impacts in these categories are extremely concerning. Online harms contribute to LGB+ people's ability to live freely. Their close relationships and sexual autonomy can already be limited because of homophobic views that limit their freedoms, which, when amplified online, compound the negative impacts on LGB+ people. Their physical safety can be at risk because of homophobic laws in some countries and discriminatory social norms held by certain groups (Human Rights Watch 2020; Sallam 2018; Gritten 2022), and this data shows that their physical safety and their desire to live are worsened because of online harms.

LGB+ people (19.3 percent) were more likely than heterosexual people (13.5 percent) to face chronic attacks that happened a few times, monthly, weekly or daily. As organized online attacks against LGB+ people become more common, the online harms against LGB+ people become more relentless and difficult to escape. Efforts to end online harms must focus on the needs of this particular community.

LGB+ people reported high rates of being targeted for their gender identity (28.7 percent), gender expression (17.8 percent) and sexual orientation (42.7 percent) compared to heterosexual people. This reflects the research mentioned above where a person's marginalized identity factors are often directly linked to the form and substance of online harms, where abusers purposely use discriminatory language related to a person's inherent identity.

Women

Overall, women reported slightly higher prevalence of any form of online harm (59.9 percent) than men (57.0 percent). In the two most common categories of online harm, repeated unwanted contact and unsolicited sexual images, women reported a significantly higher proportion of incidents (39.4 percent and 28.9 percent, respectively) than men (31.3 percent and 22.8 percent, respectively). Men reported similar or slightly higher proportions of incidents in the other forms of online harm. Among all genders, men were by far the most common perpetrators of online harms, in particular when it was a woman who was targeted.

Despite having similar numbers of incidents of online harms in many categories, women reported higher rates of negative impacts in almost all categories compared to men. They reported higher levels of impact to mental health (29.4 percent versus 21.8 percent for men), ability to engage freely online (22.9 percent versus 18.6 percent), ability to focus (19.8 percent versus 16.3 percent), physical

safety (20.7 percent versus 16.3 percent), desire to live (15.8 percent versus 13.6 percent) and sexual autonomy (16.8 percent versus 14.6 percent). Men only ranked higher than women in the negative impact on their employment and business (17.5 percent for men versus 15.9 percent for women, although not statistically higher). This reflects previous studies on online harassment and intimate image sharing that show that while men may report similar or higher levels of TFV, the impact on women is worse (Vogels 2021; Henry et al. 2020). This shows the gendered inequality women face, as they experience increased harms when targeted by TFV. TFGBV is a serious concern for women, who more and more are feeling unwelcome in digital spaces due to increased sexism and violent threats against them. This compounds the discrimination they experience in the physical world, amplifying discriminatory norms and making them feel increasingly unsafe.

Women reported higher rates of negative impacts from online harms in almost all categories compared to men.

Women were much more likely to report being targeted by their gender identity (29.8 percent) than men (16.0 percent). They reported lower numbers in other categories such as race, religion and disability than men, which could suggest that many women believe they are primarily targeted because of their gender identity, even though aspects of a woman's identity such as her race and sexual orientation have been shown to be intersecting factors in why a woman might be attacked online.

Identity-Based Discrimination and Intersectionality

Regardless of gender, most participants reported at least one identity factor as the reason that they were targeted with the most serious form of online harm they experienced. Only 37.4 percent said that no identity factor was the reason that they were targeted. Gender identity, gender expression, race, ethnicity, age, sexual orientation, religion and disability were listed as reasons that people were attacked in the majority of the most serious incidents of online harm. Factors that have been recognized to relate to human rights abuses, such as attacks on people because of their marginalized identity factors, including gender, sexual orientation, race, religion and other factors, are directly linked to the majority of online harms.

Public Perception

Public perception of women and LGBTQ+ people having more negative experiences with online harms was apparent in the data. When asked about their perceptions of OGBV specifically, respondents were much more likely to report that it was a problem for LGBTQ+ people (46.5 percent) and women (44.3 percent) than for men (22.7 percent). Public perception about OGBV showed that around twice as many people thought that the current online atmosphere was more negative for women and LGBTQ+ people. As witnesses to OGBV, the public reports there is a higher negative impact for groups marginalized by their gender and sexual orientation.

When asked about their general perceptions about online harms, there was a difference among men, women and LGBTQ+ people. Despite reporting similar or higher proportions of incidents of online harm in many categories, men consistently rated almost all forms of online harm as less harmful than women, which reflects much of the research discussed above that shows that women are more negatively impacted by TFV than men. Surprisingly, transgender and gender-diverse people rated most forms of online harm as less harmful than men and women even though as individuals they reported more incidents of harms and more serious impacts than most other groups. This unusual contrast may be due to a normalizing effect, where people who experience online harms more regularly may start to downplay its overall effects because the experience is so common and because they receive so little public support for the harms they experience. The data from this survey shows a similar pattern with young people, who experience higher proportions of online harms and are personally more negatively impacted by most categories of online harms, yet also rate it as less harmful than older populations. Some consistency of this pattern was also found with

LGB+ people, where a similar or smaller proportion of LGB+ respondents rated some forms of online harm as less harmful compared to heterosexual respondents, despite experiencing a higher prevalence of online harm in several categories. The harms faced by transgender, gender-diverse, LGB+ and young people may be downplayed by the larger society in ways that impact their general conceptions of these harms. This potential normalization of TFV among those groups that are most impacted is a disturbing trend.

Perpetration

Of the most serious incidents of online harm reported, 24.8 percent reported that they did not know the gender of the person who targeted them.

Despite many people not being able to identify the gender of their perpetrator, gender appeared prominently in who was the perpetrator inflicting the online harm among those who could identify the gender of their perpetrator. Men stood out as the gender of the person causing most harmful incidents of online harm a person experienced. Almost half of people (49.7 percent) reported that men caused the most serious incident of online harm they experienced, the highest percentage in all gender categories. The gender of the target also showed a gendered pattern, with women (57.7 percent) and transgender and gender-diverse people (51.6 percent) reporting being targeted by men at higher numbers than men (42.9 percent), who still reported that men were the primary perpetrators of the most serious incident of online harm they experienced.

Women were much less likely to be the person causing the most serious harm. Among people who had experienced some form of online harm, 18.9 percent reported that a woman had been the perpetrator. Men (23.1 percent) and transgender and gender-diverse people (25.8 percent) were more likely to report that a woman had targeted them compared to women (18.1 percent).

Few transgender and gender-diverse people were reported as perpetrators. Only 1.1 percent of all participants who had experienced online harms reported that a person of an "other" gender targeted them.

Responding to TFGBV requires not only providing supports to those who are victims/survivors of TFGBV, but also changing the behaviour of those perpetrating the harms. The data from this survey demonstrates that men and boys are responsible for a significantly higher percentage of harms compared to trans and cis women and gender-diverse people. As such, supports to respond to TFGBV must include efforts to change the behaviour of men and boys online.

Almost

of people reported that men caused the most serious incident of online harm they experienced, the highest percentage in all gender categories.

Section II

Supports and Resources

The following section discusses various existing supports and resources available to victims/survivors of TFV, as well as where there are gaps and barriers in finding support. It then summarizes survey participants' perceptions of and experiences with accessing these supports and resources.

Introduction: Supports and Resources

As the prevalence of TFV increases, victims/survivors need support and resources to help address and prevent the abuse they are facing. There is also a need for resources to address this issue systemically to eradicate it. These supports and resources can come in the form of content moderation on and by social media platforms, educational resources on TFV, technical solutions, governmental and non-governmental victim/survivor support programs, research, and robust and evidence-based laws and policies. Support and resources should help a victim/survivor when they have been a target of TFV but should also be preventive in nature. Research and education can help shape the social norms of what is and is not appropriate behaviour in digital spaces and address the underlying discriminatory beliefs that fuel TFV.

To date, many victims/survivors of TFV report struggling to find adequate support when they are harmed by TFV. From a legal perspective, depending on the country a person lives in, there will be varying levels of criminal or civil laws that are applicable to TFV. However, even when relevant laws are in place, victims/survivors may face barriers in accessing those legal remedies, due to systemic bias and failures within the legal system, as well as challenges with affordability and other access to justice issues. Content moderation can be a helpful and time-sensitive tool for getting harmful content taken off websites and managing TFV, but how each company's terms of service are applied to complaints can be confusing, unclear and inconsistently applied. The types of behaviour and content that are forbidden on a platform can vary widely. Additionally, the rules might not be available in all languages and the policies might not be culturally relevant to people in the Global South.

To date, no social media company has come up with a sufficient system to address TFV and most do not provide adequate resources to tackle this issue, leaving many victims/survivors without redress. Governmental and non-governmental digital rights or victim service organizations have proven useful to victims/survivors in some cases, but they are few and far between in most countries. Education and support tools can also be a practical resource for people to learn about topics such as privacy, online safety, digital etiquette and what actions are available for people to respond to and prevent TFV, but there are relatively few governments and organizations directly providing this type of information in an accessible format. Finally, research can help identify trends and practices related to TFV and determine what actions are best suited to prevent and address TFV. In the past few years, there has been a great deal of research conducted on this subject, but more is needed, particularly in the Global South.

Background: Supports and Resources

Government Support

Governments must support efforts to end TFV. In some countries, governments are taking steps toward addressing this issue; however, in others, governments are working actively against the rights of women and LGBTQ+ people and are not taking TFV seriously. As noted above, some governments and leaders are even engaging in TFV themselves. In many countries, laws have been used to suppress women's and LGBTQ+ people's legitimate digital interactions, including their advocacy for human rights and sexual expression. For example, at the time this report was written, as Iranians protested for women's rights, the government implemented strict internet controls limiting protesters' abilities to communicate with each other and spread their message with the world (Green 2022). In several countries, obscenity and decency laws have been used to penalize women's online sexual expression (Global Information Society Watch 2017) or advocacy for sexual and reproductive rights (Palumbo and Sienra 2017). Governments must not limit women and LGBTQ+ people's legitimate sexual expression and advocacy. Instead, they should be developing — and funding — human rights-based research and supports to end TFV.

Several countries have developed government supports for victims/survivors of TFV. Some countries have even created statutorily empowered bodies whose function is to address TFV. Others have provided government support for programs such as helplines for victims/survivors of TFV. Governments need to continue developing human rights-based supports and providing resources to those organizations and researchers that can best support victims/survivors of TFV.

Research by Pam Hrick (2021, 595) has shown that statutorily empowered bodies "have the potential to meaningfully further a survivor-centered approach to combating technology-facilitated violence against women — one that places their experiences, rights, wishes, and needs at its core." Hrick reviewed the work of Australian eSafety Commissioner, New Zealand's Netsafe, and two Canadian bodies, the CyberScan unit in Nova Scotia and the Canadian Centre for Child Protection in Manitoba. She found that these bodies, while not perfect, provide victims/survivors with a variety of legal and non-legal options to address TFV. Hrick noted that these bodies demonstrate a commitment from governments that they are trying to take TFV seriously.

In Australia, the Office of the eSafety Commissioner provides direct supports to survivors/victims of TFV in getting content removed from the internet.[116] It also conducts research; develops educational materials; and engages with social media, messaging, gaming and app services, and websites, to ensure those companies are working to keep Australians safe online. In New Zealand, Netsafe investigates complaints, provides mediation, liaises with social media companies to request the removal of harmful content and develops educational tools to inform New Zealanders about online safety.[117] In the Canadian province of Nova Scotia, CyberScan is mandated to provide dispute-resolution services for victims/survivors, information on legal rights and education on TFV.[118] Research by Alexa Dodge (2021) found that most people who use this service are interested in the non-legal technical and emotional supports, and are often able to resolve their issue without engaging in the legal system; however, some do seek legal information supports from CyberScan. In Manitoba, the Canadian Centre for Child Protection provides supports to people who have had their intimate images shared without consent.[119]

Other governments have provided supports to organizations assisting victims of TFV. In the United Kingdom, the government helps fund the Revenge Porn Helpline.[120] Adults who have had their intimate images shared online without consent can call this helpline for assistance in getting the images removed.[121] In South Korea, the Ministry for Gender Equality funds the Centre for Online Sexual Abuse (McGlynn, n.d.). In India, a women's helpline is available for women to make complaints, including those related to TFGBV (Kovacs 2017).

These types of supports are vital to victims/survivors of TFV, who deserve to have immediate and accessible government-backed help with legal and non-legal options to respond to their experiences. Governments play a key role in funding and supporting independent and civil society organizations and initiatives that provide human rights-based services and conduct research on TFV, in particular for equity-seeking groups.

International initiatives can also help curb TFV globally. In recent years, several international partnerships have been created to work toward a better understanding of TFGBV and to strategize how best to tackle the issue. The Global Partnership for Action on Gender-Based Online Harassment and Abuse was launched in 2022 (Crockett and Vogelstein 2022). The partnership includes Australia, Canada, Chile, Denmark, Iceland, Kenya, Mexico, New Zealand, South Korea, Sweden, the United Kingdom and the United States (Global Partnership for Action on Gender-Based Online Harassment and Abuse, forthcoming 2023). It "will bring together countries, international organizations, civil society, and the private sector to better prioritize, understand, prevent, and address the growing scourge of technology-facilitated gender-based violence" (US Department of State 2022). A Global Online Safety Regulators Network was established "with the aim of making sure the approach to online safety between countries is as consistent and coherent as possible."[122] This network includes representatives from Australia, Fiji, Ireland and the United Kingdom. Global partnerships like these have the potential to be beneficial as they can share existing knowledge and help develop and advocate for laws and policies to address TFV.

116 See www.esafety.gov.au/.

117 See https://netsafe.org.nz/.

118 See https://novascotia.ca/cyberscan/.

119 See www.protectchildren.ca/en/.

120 See www.gov.uk/government/news/revenge-porn-helpline-launched-by-government.

121 See https://swgfl.org.uk/helplines/revenge-porn-helpline/.

122 See www.esafety.gov.au/about-us/who-we-are/international-engagement/global-online-safety-regulators-network.

Legal Responses

State recognition of the harms caused by TFV plays both an expressive (Citron 2009) and practical role (Franks 2015) in addressing TFV. When governments develop laws that prohibit TFV, it signals to the public the state's condemnation of these types of behaviour, and it also provides a legal avenue for victims/survivors to seek a remedy from the state.

Certain forms of TFV, such as NCDII, may require the creation of new laws, but in many jurisdictions, existing laws can already be applied to many forms of TFV (European Institute for Gender Equality 2022). TFV can be a new manifestation of harms that are already recognized by the state, and those laws should apply regardless of whether the harm occurred in a digital or physical space. As noted by Jane Bailey and Carissima Mathen (2019), in the Canadian context, existing criminal laws, such as harassment and extortion, can apply to forms of TFV, as well as specific laws such as criminal voyeurism or NCDII. Suzie Dunn and Alessia Petricone-Westwood (2018) found a similar trend in civil responses in Canada, where many existing civil laws could be applied to TFV, but additional civil statutes and torts that directly address TFV were also beneficial. However, TFV-specific laws are lacking in many countries (Machirori 2017) and there is significant under-reporting of these harms to legal authorities even when there are laws in place (Malanga 2021; Nwaodike and Naidoo 2020). Catherine Muya's (2021) research on TFGBV in Kenya found that the laws in that country needed to be revised to properly address TFGBV and many women were left with no legal remedy due to the lack of legislation on the issue.

Several countries have created laws to address NCDII (Kamran and Ahmad 2021). In 2018, Natália Neris, Juliana Pacetta Ruiz and Mariana Giorgetti Valente conducted a comparative analysis of countries that have introduced such laws. At that time, they found that 11 countries had specific NCDII laws[123] and 21 had general laws, such as laws against harassment, gender-based violence and domestic violence, that could apply,[124] and several had bills and public policies in place.[125] In 2009, the Philippines was one of the first countries to criminalize NCDII. Neris, Ruiz and Valente (2018) noted that of the countries that introduced NCDII laws, most countries had introduced criminal laws, but some countries did have civil laws to address NCDII. Research by Aikenhead (2018) on Canadian criminal cases involving NCDII and by Bailey and Mathen (2019) on those involving other forms of TFGBV show that there is a significant gendered trend in these cases, with most victims being women and most offenders being men

When governments develop laws that prohibit TFV, it signals to the public the state's condemnation of these types of behaviour, and it also provides a legal avenue for victims/survivors to seek a remedy from the state.

A study by Neris, Ruiz and Valente (2018) found that most NCDII laws did not address whether internet intermediaries could be held liable for the role they played in the dissemination of the images or require them to take action to get content removed. Only a few jurisdictions, such as Australia, included potential fines for companies that refused to remove content.

Even in countries that have developed laws to address TFV, many people report that there are barriers in getting an adequate legal remedy and believe that the legal system is failing women and LGBTQ+ victims/survivors of TFV. Law enforcement

123 Australia, Canada, France, Israel, Japan, New Zealand, the Philippines, Scotland, Spain, the United Kingdom and the United States.

124 Argentina, Australia, Brazil, Cameroon, Canada, Chile, Colombia, Denmark, Germany, India, Japan, Kenya, Malawi, Portugal, Puerto Rico, South Africa, Spain, Uganda, the United Kingdom, the United States and Uruguay.

125 Argentina, Australia, Brazil, Chile, Denmark, Mexico, Portugal, Puerto Rico, South Africa, the United States and Uruguay had bills, and Australia, Canada, Denmark and New Zealand had public policies.

officers have minimized gender-based violence (Mahmutović, vale and Laçí 2021) or examined the case from a "patriarchal-protectionist way" (Devika 2019, 12). Further, harms experienced in digital spaces may not be taken as seriously as physical violence by some police officers (Gurumurthy and Vasudevan 2018; Mahmutović, vale and Laçí 2021). Under-reporting of these harms was also common. For example, women in Ethiopia, Kenya, Senegal, South Africa and Uganda often did not report TFGBV to law enforcement and when they did, some of their complaints were trivialized by law enforcement (Nwaodike and Naidoo 2020). Gender discrimination that minimizes violence against women and blames the victim was a common trend for people reporting TFGBV to police globally (Nguyen and Barr 2020; Dodge et al. 2019; Devika 2019; Sequera 2021). A lack of training (Segal 2015) and discriminatory responses by police (Powell and Henry 2016) were some of the reasons that some research found that law enforcement was failing victims of TFGBV (Machirori 2017). Some actors in the legal system may be lacking the skills needed to understand and properly address TFV and require additional training (Dunn and Aikenhead 2022). In the civil context, seeking a civil remedy may be unaffordable for some and the response may be too slow to provide an adequate remedy (Young and Laidlaw 2020; Nwaodike and Naidoo 2020). Further, some victims/survivors may be reluctant to report because of potential negative social consequences related to patriarchal and sexist norms in their community (Malanga 2020).

Additionally, in some countries, existing laws that regulate sexual expression, identity or orientation can actually hinder some victims'/survivors' ability to access justice, express their sexuality or engage in activism. In many countries, LGBTQ+ people are at risk because same-sex relationships are criminalized and gendered dress codes are enforced.[126] In countries such as Japan, Malawi and Uganda, obscenity and anti-pornography laws criminalize some forms of sexual imagery, which, according to Neris, Ruiz and Valente (2018, 41) "raise questions about the risk of increasing the vulnerability of victims that may end-up being punished instead of protected." Sarai Chisala-Tempelhoff and Monica Twesiime Kirya (2016) report that anti-pornography laws and anti-obscenity laws are in place in Uganda and Malawi to regulate sexuality and control women's bodies and sexual expression. Some victims/survivors of NCDII have been charged under these laws when their images were shared without consent. In Canada, the United Kingdom and the United States, young people have been warned, and some have been criminally charged, with taking or sharing intimate images of themselves as a form of child sexual abuse material production, regardless of whether it was consensually made and shared or not, for example, when an older adolescent takes a nude photo of themselves and the image is never used in an exploitative manner (Hasinoff 2014; Karaian 2013; Miles 2020; Dodge 2021). These cases show that some existing laws have the potential to be used against people who have been victimized by TFV or can criminalize legitimate sexual expression.

Another important legal issue to address is anonymity and privacy (Hernández 2017). At times, it can seem that there is a tension between protecting victims/survivors of TFV and protecting anonymity and privacy. However, anonymity and privacy are important factors in keeping people safe from TFV. Many women, LGBTQ+ people and human rights defenders communicate online using anonymity and encryption to protect themselves from harassment and abuse (Yahaya and Iyer 2022; Hernández 2017). As such, these are important aspects of digital communication to protect. Additionally, in legal cases involving private sexual content, victims/survivors need anonymity to bring their cases forward (McGlynn 2016). If there is a possibility that their name and the associated content could be shared publicly, victims/survivors may be reluctant to report out of fear that the content and details will be viewed and spread further.

Anonymity can create challenges for victims/survivors of TFV. Some victims/survivors may not know the identity of the person who has targeted them and may need support from law enforcement to find out (Dunn and Aikenhead 2022). However, when governments create laws that assist them in unveiling a person's identity in digital spaces, they must take into account the fact that anonymity and privacy are important factors related to online safety and freedom (Treuthart 2019). Any government powers that impact privacy and anonymity should be legally justified, limited and narrow. Human rights such as privacy must be taken into consideration. TFGBV should not

126 See www.ohchr.org/en/sexual-orientation-and-gender-identity/about-lgbti-people-and-human-rights.

be co-opted as a reason to create overly broad government powers that can unjustly infringe on privacy and freedom of expression (Access Now 2021). As noted by Citizen Lab and the Canadian Internet Policy and Public Interest Clinic, any laws created that impact these issues must utilize a human rights-based approach to fairly balance people's right to privacy and expression with government interests such as public safety and national security (Gill, Israel and Parsons 2018).

Technology Companies

Technology companies play an essential role in preventing and responding to TFV. Their products and services are the very platforms and devices that host and facilitate TFV. The level of commitment these companies have for addressing TFV determines the safety and well-being of billions of people worldwide. At this time, many people question technology companies' commitment to properly address TFGBV and TFV against LGBTQ+ people and other equity-seeking groups. Many of these companies' track records are questionable at best. For example, at the time this report was written, Elon Musk, the current owner of Twitter, had recently allowed several banned misogynist, racist, violent and transphobic users back onto the platform in the name of free speech (Milmo 2022) and dissolved Twitter's Trust & Safety Council (Mehta 2022). Although this is a starker example of problematic choices by a social media company, most technology companies' corporate motives are geared toward encouraging user engagement to increase profits and there is less incentive to provide robust content moderation and safe products, which impact their profit margins (Zuboff 2019; Goldberg 2019). Additionally, Pollicy has noted that social media companies' content moderation practices prioritize Western values and can be biased against racialized people and in the African context (Iyer et al. 2021).

As noted by Bailey et al. (2021), social media companies also engage in structural violence in which AI content sorting and algorithmic profiling reinforce existing stereotypes about equity-seeking groups, provide biased and discriminatory outcomes, and create disparate access to information on their platforms. Algorithms can cause additional harms when they prioritize and serve up content on tech platforms that promotes extremist sexist, racist and homophobic content (Ribeiro et al. 2020). It is essential that technology companies commit to ending TFV on their platforms and devices by committing resources and developing best practices.

Most social media companies do have content moderation rules and terms of services that prohibit various forms of TFV and have tools for preventing abuse (Khoo 2021). In Danielle Keats Citron's book, *The Fight for Privacy*, she discusses some of the positive advancements social media companies have made, in part due to pressure and engagement with academics, law makers and anti-violence advocates, while recognizing that there is a long way to go (Citron 2022). Citron describes the early work done by the Cyber Civil Rights Initiative and the US Cyber Exploitation Task Force, which advised law makers and large technology companies such as Google, Twitter, Meta (Facebook at the time) and Tumblr to improve their policies and laws. The work of these types of groups has played an important role in encouraging social media platforms to improve their policies and practices. For example, the Revenge Porn Helpline has worked with companies, including Meta, to promote tools that help prevent the spread of intimate images,[127] while the dating app Bumble has developed a blurred image feature that uses AI to detect sexual images in response to complaints about unsolicited nude images on their apps, allowing users to decide whether to view the images or not.[128] Many victims/survivors of TFV use technical tools on these sites, including blocking and reporting harmful content, to prevent future abuse (Iyer, Nyamwire and Nabulega 2020; Kovacs, Padte and SV 2013).

Although content moderation rules exist on most popular social media sites, many victims/survivors of TFV remain dissatisfied with these companies' overall responses to TFV (Dhrodia 2018; Ruiz, Valente and Neris 2019). Internet Sans Frontières (2019) found a low level of reporting (15 percent) of TFGBV to social media companies among women in West and Central Africa, which suggests that individuals may not believe that these organizations will adequately respond to complaints, or that companies have not made

127 See stopncii.org.

128 See https://bumble.com/en/help/why-am-i-seeing-a-blurred-image.

their users aware of their content moderation systems. APC conducted a report on improving corporate policies to end TFGBV (Athar 2015). It found that while companies did have some policies in place to address TFGBV, there was "little to no public information…available about how internal review processes work" (ibid., 20) and a great deal of harmful content remained online due to inconsistent policies and application of those policies. There were also barriers to some people who could not find help-seeking information in their language.

The LEAF report *Deplatforming Misogyny* (Khoo 2021) outlined many of the challenges and barriers women and LGBTQ+ people faced when reporting to social media companies. Khoo found that content moderation policies could be opaque and inconsistently applied. Social media companies were more likely to address harmful content when there were negative media reports about the content that drew attention to it, rather than address it consistently. LEAF noted that the business models of these companies focus on user engagement, regardless of whether that engagement is positive or negative, thus disincentivizing those companies to remove content that engages users, even if it may be harmful. LEAF proposed an equality-focused and human rights-based approach to regulating social media companies' content moderation practices that would better protect victims/survivors of TFGBV. Many other organizations, such as the Internet Democracy Project (Bhandari and Kovacs 2021), APC (Athar 2015) and IT for Change (Gurumurthy and Dasarathy 2022), have called for improvements in platform governance to address TFGBV. As noted by Suzor et al. (2019), social media companies have a responsibility to prevent TFGBV on their platforms.

Civil Society Organizations

As mentioned in the section on the expert advisory committee, civil society organizations have been at the forefront of this issue for nearly two decades. Much of their research and advocacy was what brought this issue to the attention of governments and the public. Organizations such as APC, Derechos Digitales, the Internet Democracy Project, the Digital Rights Foundation, Amnesty International, the Cyber Civil Rights Initiative, GLAAD, the National Network to End Domestic Violence and the BC Society of Transition Houses have been conducting research, developing information and education on TFV, and providing reports and resources to victims/survivors for years. These organizations are essential in the ecosystem of stakeholders who are committed to ending TFV. However, there are relatively few civil society organizations doing this work and many of them are underfunded.

Civil society organizations are often the first place that victims/survivors find information about their rights and have their experiences validated as a violation of their rights. For example, the Digital Rights Foundation provides a helpline in Pakistan that people can call if they are harassed online.[129] These organizations assist with formal and informal responses to TFV, advise governments and social media companies on how to improve their laws and policies and, most importantly, feature the voices of victims/survivors of TFV.[130] The value of their work cannot be underemphasized. Institutions like these that centre gender equality, the rights of LGBTQ+ people and human rights have filled the gaps in countries where legal or governmental supports are lacking (Muya 2021). However, they often work with limited funding and supports. Additionally, traditional anti-violence organizations have had to quickly catch up to the novel issues that their clients experience when their abusers use technology to harm them (National Network to End Domestic Violence 2014; AWARE 2020). These organizations should be supported and adequately funded by governments so that they can continue doing their essential work and provide non-legal avenues for victims/survivors.

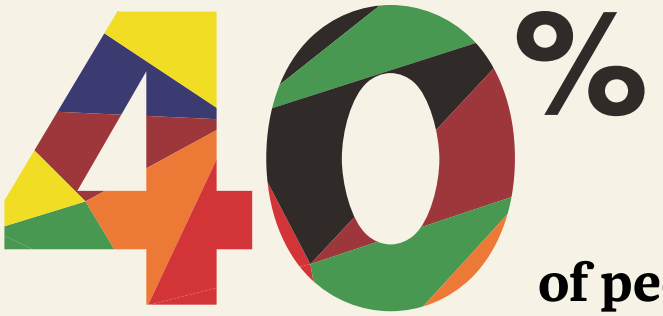
Research

As noted by the International Center for Research on Women, the concept of TFGBV is still being developed and understood (Hinson et al. 2018). There is a growing number of researchers working in this area in academic and civil society circles. There is a need for additional data collection and analysis on this subject for this issue to be better understood, in particular information

129 See https://digitalrightsfoundation.pk/contact/.

130 See https://cybercivilrights.org/.

Almost



of people did not reach out to anyone about the most serious incident of online harm they experienced.

gathered from people who have experienced TFV (Global Partnership for Action on Gender-Based Harassment and Abuse, forthcoming 2023). APC stated, "more systematic documentation of [TFGBV], including in-depth case studies, is necessary to identify effective remedies and new policies" (Fascendini and Fialová 2011, 54), including consultations with organizations that do work on TFGBV. It further noted that, "particular attention should be given to women marginalised due to race, sexual orientation, intellectual and physical abilities, age and socio-economic factors such as geographical location, level of education, employment situations, and marital status" (ibid.). Additionally, policies and practices aimed at ending TFV should be evidence based. As noted by Hrick (2021, 599), any actions to address TFV should be "informed by research, evidence and the perspectives of survivors."

Education

Education campaigns play multiple roles in ending TFV (European Institute for Gender Equality 2019). They can help inform victims/survivors about what their rights are (APC & Humanist Institute for Cooperation with Developing Countries 2013) and provide them with information on how to protect themselves and manage their experiences with TFV (YWCA Canada 2015).131 For example, in Africa, Open Internet for Democracy has noted that there is a need for more educational campaigns about TFGBV so women and girls can understand their rights to safety and privacy online (Malanga 2020). In a multi-country study in Asia, UN Women found that there was a lack of digital literacy among women that impacted their safety online (Aziz 2020). Education campaigns can also be used to educate legal actors on best practices in addressing TFV, as many law enforcement officers lack training and understanding on TFV (Shariff and Eltis 2017, 110; Dunn and Aikenhead 2022). Research by the Centre for Development Studies in India found that research on TFGBV is limited and more reliable country-specific data is needed to better inform individuals and law enforcement (Devika 2019). Additionally, education can play a preventive role by working to change people's behaviour online, including that of perpetrators. This can be done by providing information on what healthy digital interactions should look like and challenging the root causes of TFV, such as sexism, homophobia, transphobia, racism, ableism and colonialism.

The task of addressing, responding to and preventing TFGBV will take a multi-stakeholder approach that provides a variety of remedies and supports for victims/survivors, as well as a combined effort by law makers, educators, researchers, individuals, civil society organizations and technology companies.

131 See https://hackblossom.org/cybersecurity/.

Survey Results: Evaluation of Supports and Resources

The following section examines participants' opinions on supports and resources.

Participants were asked on a five-point scale with 5 being "very important" and 1 being "not important at all" how important certain resources and supports were in addressing OGBV.

The following information includes those that rated these categories as "very important." As such, those that listed these resources and supports as moderately important or not important at all are not included in these numbers. Nearly half or more reported each category as a very important resource or support.

When participants were asked about what resources would be most helpful to address OGBV, they identified tools for awareness: 57.5 percent reported education campaigns in schools as very important, 57.4 percent reported information on how to protect themselves online as very important, and 52.9 percent reported public education campaigns as very important.

When asked about legal and policy resources, 60.2 percent reported laws as very important, 54.4 percent reported police as very important, and 53.6 percent reported government support as very important.

When asked about tools for support, 53.1 percent reported technical supports for internet security as very important, and 52.1 percent reported helplines as very important.

When asked about non-governmental resources: 50.1 percent reported content moderation by social media companies as very important, 51.2 percent reported OGBV organizations as very important, and 45.2 percent reported civil society organizations as very important.

Survey Results: Effectiveness of Supports and Resources

Participants were asked to rate which resources and supports they generally considered effective in responding to OGBV on a five-point scale, with 5 being "very effective" and 1 being "very ineffective."

The following information includes those who rated these categories as "very effective" of participants who provided a rating.

When participants were asked about what resources were most helpful to address OGBV, 38.1 percent rated information on how to protect themselves online as very effective, 35.0 percent rated education campaigns in schools as very effective, and 31.2 percent rated public education campaigns as very effective.

When participants were asked about what resources were most helpful to address OGBV, 35.1 percent rated internet security as very effective, and 31.8 percent rated helplines as very effective.

When participants were asked about what resources were most helpful to address OGBV, 35.5 percent reported laws as very effective, 32.9 percent reported police as very effective, and 30.4 percent reported government support as very effective.

When participants were asked about what resources were most helpful to address OGBV, 29.6 percent reported content moderation by social media companies as very effective, 31.5 percent reported OGBV organizations as very effective, and 26.5 percent reported civil society organizations as very effective.

Survey Results: Who Has Responsibility to Act?

When asked to rate which organizations have the most responsibility to address OGBV, respondents were most likely to rate police (23 percent) as having the highest responsibility, followed by governments (19.4 percent), law and policy makers (17.8 percent), social media companies (15.2 percent), schools and universities (9.6 percent), other internet users and community members (9.8 percent), and civil society organizations (5.2 percent).

Survey Results: People/ Organization Reached Out to Following the Incident

When considering the most serious incident of online harm they had experienced, most people did not reach out to anyone (39.6 percent) about the incident. Friends (24.1 percent), family members (17.7 percent) and spouses/partners (10.2 percent) were the most common people reached out to.

Formal reporting mechanisms such as reporting to the police (10.1 percent), social media companies (8.4 percent), lawyers (4.9 percent), governments (4.0 percent), schools/universities (4.0 percent) and employers (3.0 percent) were much less commonly used.

Community-based supports such as helplines (4.9 percent), mental health workers (5.0 percent), civil society organizations (2.8 percent), faith-based organizations (2.7 percent), victims support organizations (2.7 percent), or doctors and health-care workers (2.9 percent) were also less commonly used to report experiences of online harm.

Survey Results: Effectiveness of Resources

When asked how effective the person or organization was in helping them with their most serious incident, participants were asked to rate the effectiveness on a four-point scale, with 4 being "very effective" and 1 being "completely ineffective."

Close relationships were most likely to be considered very effective: nearly half of the respondents rated spouses (49.7 percent), family members (48.3 percent) and friends (41.0 percent) as very effective.

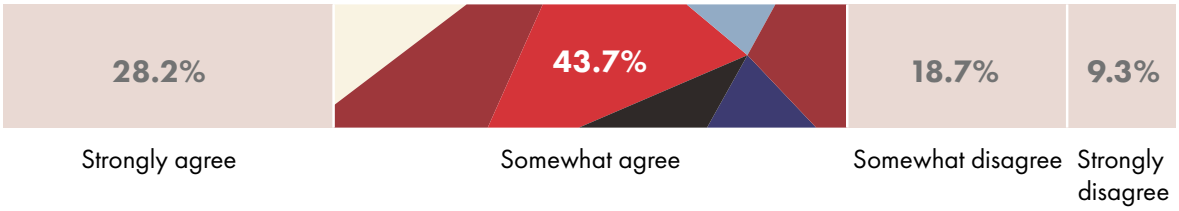
Community-based supports followed as next most commonly rated as very effective, where respondents rated helplines (29.8 percent), mental health workers (39.4 percent), civil society organizations (32.2 percent), faith-based organizations (37.5 percent), victims support organizations (36.7 percent), or doctors and health care workers (39.6 percent) were rated as very effective.

Formal mechanisms were less commonly rated as very effective, where police (28.8 percent), social media companies (22.4 percent), lawyers (34.0 percent), governments (26.3 percent), schools/universities (25.9 percent) and employers (30.1 percent) were rated as very effective.

Survey Results: Personal Skills

Participants were asked on a four-point scale whether they had the skills or knowledge to help someone they knew who had experienced OGBV.

Figure 1: Have Skills or Knowledge Needed to Help Someone Who Has Experienced an Incident of OGBV



Summary of Survey Results: Supports and Resources

Many participants reported that they had some skills or knowledge to help someone they knew who had experienced OGBV. Most people either strongly agreed (28.2 percent) or somewhat agreed (43.7 percent) that they had some skills or personal knowledge to help people targeted by OGBV. As most people do not seek formal supports when experiencing TFGBV, providing educational material and technical supports to those who are helping someone could go a long way in supporting victims/survivors of TFGBV. However, formal supports are also essential when they are effective and accessible.

Participants of this study found a variety of supports and resources to be very important. Approximately half of all participants identified educational campaigns, legal and policy resources, tools for support and non-governmental resources as very important resources. This data show that victims/survivors of online harms are interested in a variety of responses to online harms, which supports the argument for a multi-stakeholder approach to addressing, responding to and preventing online harms.

Unfortunately, the effectiveness of the resources surveyed was rated relatively low by participants, demonstrating that there is a need for increased investment in supports and resources to address TFV. Among participants, information on how to protect themselves online (38.1 percent), laws (35.5 percent), education campaigns in schools (35.0 percent) and police (32.9 percent) were most likely to be rated as "very effective," although most other resources were close in rating (between 26.0 percent and 31.2 percent). Participants also identified police (23.0 percent) and governments (19.4 percent) as the organizations with the most responsibility to address OGBV, demonstrating that there is a desire for legal and governmental intervention into these issues.

Of those that had experienced at least one form of online harm, when considering the most serious incident they experienced, a shocking number of people did not tell anyone about the incident, not even family and friends. Specifically, 39.6 percent of people did not seek out any supports or resources and managed the incident alone. Victims/survivors of online harms should not have to suffer alone and should be able to seek help from members of their community, government, technology companies and civil society supports. The fact that victims/survivors are not telling people or organizations about their experiences may suggest that existing supports and knowledge are lacking or that people may not be aware of, or not have faith in, those that do exist. As noted in the background section, there is a growing movement of government and non-governmental supports for victims of TFGBV, but they are relatively rare internationally. There is a need to improve and increase these services, make people aware of them and monitor their effectiveness.

Victims/survivors were most likely to seek out informal supports through close relationships such as friends (24.1 percent), family members (17.7 percent) and spouses/partners (10.2 percent). If victims/survivors of online harms are seeking informal supports, it is essential that supports and resources, such as educational information and information about how to address online harms, be available to the public so that they can support their loved ones when they come to them for help.

Formal mechanisms were less commonly accessed. Only 10.1 percent sought help from police and only 8.4 percent sought help from social media companies. It must be remembered that this is in response to the most serious incident of online harm they experienced. This under-reporting of online harms suggests that there may be a lack of accessible and responsive formal supports for victims/survivors, including legal options for victims/survivors. Previous research shows that TFV is not taken seriously by all legal actors; in some countries, laws may not be in place to protect people from some online harms, and certain individuals and communities lack trust in the justice system to respond to crimes committed against them. Additionally, some online harms may not reach a legal threshold and a non-legal response would be more appropriate. The lack of reporting to social media companies also suggests that current social media policies may be inaccessible or perceived as unhelpful, as reflected in previous research mentioned above. It may also suggest that there is a lack of education by social media companies on how to seek out supports from social media companies. Formal supports are especially important for more serious forms of online harm

that require an immediate response, as they risk being amplified and spread online over time prior to a formal remedy.

When rating the effectiveness of these supports and resources, participants rated their informal support systems as most effective. Spouses/partners were most rated as very effective (49.7 percent), followed by family members (48.3 percent) and friends (41.0 percent). Although community-based supports were some of the least commonly accessed supports or resources, they were more commonly rated as more effective than formal mechanisms such as police (28.8 percent) or social media companies (22.4 percent). Community-based resources such as doctors and mental health workers (39.6 percent) and victim support organizations (36.7 percent) were more commonly rated as very effective. This data shows that in practice, community-based organizations are providing proportionately more effective resources and supports. More resources should be provided to these types of organizations, as there are relatively few organizations that provide direct services for victims/survivors of online harms. Additionally, it suggests that there is a need for improved law enforcement practices when addressing online harms.

Conclusion

It is time to take action on TFV, particularly forms that negatively impact equity-seeking groups.

The individual and systemic harms caused by TFV perpetuate unacceptable discrimination and cause significant harms that must be addressed. The results of this study indicate that online harms are widespread, there is a lack of existing effective supports and there is a need for a multi-stakeholder effort to end TFV. Over the past two decades, TFV has only increased and, although some efforts have been made to curtail these types of harmful behaviour, currently there are inadequate resources dedicated to understanding and preventing this new form of violence. More support is needed across the world, but in particular for women and LGBTQ+ people in the Global South.

The research and data from this report predominantly represent the experiences of those in the Global South, and they demonstrate that LGBTQ+ people and women are at significant risk of experiencing online harms and being negatively affected by them. The data highlights the particularly high levels of perpetration of online harms against transgender and gender non-conforming, agender, non-binary and other gender-marginalized people who, in many countries, risk their safety and well-being when expressing themselves authentically in digital spaces. It shows that the negative impacts of online harms are most strongly felt by LGBTQ+ people and women, and that the wider community sees OGBV as a much more serious issue for these groups compared to men. As such, particular attention and resources need to be directed at these groups. Finally, it lays bare the high proportion of men who engage in this harmful behaviour, highlighting the fact that men have an essential role to play in changing their behaviour to make digital spaces safer.

The authors hope that the research, data and recommendations provided will assist in the development of a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach to social, policy, educational and technical changes. However, this data does not reveal a new story. It tells the story that civil society organizations, researchers and advocates internationally — but in particular in the Global South — have been alerting the world to for over 20 years. It is a reminder that not enough has been done and things must change to ensure that all people have access to safe digital spaces. Without action on this issue, women and LGBTQ+ people will not be able to participate equally, safely and authentically in our increasingly digital world.

The data highlights the particularly high levels of perpetration of online harms against transgender and [other gender-diverse] people.

Section III

Recommendations

The following recommendations are applicable to addressing TFV in general. However, significant attention and resources must be directed at ending TFV against equity-seeking groups who face disproportionate harms from TFV, such as members of the LGBTQ+ community, women, and racialized, disabled and young people. This includes journalists, human rights defenders and politicians from those groups and those rights defenders and politicians from those groups and those who advocate for equality and human rights. These groups face additional barriers due to the systemic oppression they face in society and the fact that their interests are often neglected or under-represented by those in power.

Additionally, specific recommendations are made for governments, technology companies, civil society organizations and researchers, think tanks and academics. Some of these stakeholders may already be engaging in the actions recommended, while some may have a way to go. Although each of these groups has a specific role to play and each has drastically different levels of influence, responses to TFV must apply an ecosystem approach, where all actors are working together toward the common goal of eradicating TFV. Those with more resources and power, such as governments and technology companies, must commit to investing in change and meaningfully engage with other stakeholders, such as civil society organizations, researchers and academics, when working to end TFV. For example, governments should fund the work of civil society organizations and researchers whose work addresses TFV. Governments should meaningfully consult and collaborate with civil society organizations, researchers, and victims/survivors when developing and implementing policies, regulations and laws. Social media companies should do the same when developing policies and content moderation practices.

With each of these recommendations, it is essential that any efforts made take a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach.

Governments

Human Rights-Based Approach

1. Take a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach when addressing TFV through laws, policies and resource distribution.

2. Engage with specialists in TFV, including civil society organizations, victims/survivors and academics/researchers, to ensure the approaches and remedies governments propose fully address the real needs of those who have been harmed by TFV, especially those from equity-seeking groups.

3. Take a clear public stance against TFV, in particular against forms that are disproportionately harmful to equity-seeking groups, such as women, girls, LGBTQ+ people, people with disabilities, Indigenous people and members of racial, ethnic and religious groups who face discrimination.

4. Ensure concepts of freedom of expression, sexual autonomy and privacy rights use a human rights-based approach. Take into consideration the silencing effect of TFV and the rights of equity-seeking groups to express themselves safely and authentically in digital spaces.

5. Address how the silencing effect of TFV undermines freedom of expression.

Collaboration and Consultation

6. Meaningfully and regularly consult and collaborate with civil society organizations, researchers, academics and legal practitioners with expertise in TFV, as well as victims/survivors, when developing laws, policies and programs related to TFV.

7. Include the perspectives and voices of diverse members of equity-seeking groups in all consultations and collaborations.

Legal and Policy Responses

8. Review existing laws that could apply to TFV to ensure that the existing structure of those laws is able to capture TFV.

9. Avoid an overreliance on criminal law solutions and ensure that there are non-criminal legal, governmental and non-governmental options available to victims/survivors, such as civil laws, privacy/data protection laws, human rights laws, administrative solutions and/or community-based solutions, that address TFV.

10. Ensure that laws do not unjustly restrict sexual expression, human rights advocacy and criticism of governments and institutions.

11. Review existing laws, such as morality, anti-pornography and anti-obscenity laws to ensure that people are not unjustly at risk of surveillance and/or criminalization or legal penalties when they create consensual and non-harmful sexually expressive material.

12. Introduce laws to address forms of TFV that are not addressed by existing laws.

13. Ensure that legal responses to TFV include timely legal orders to have harmful content removed, deleted or de-indexed from the internet when appropriate.

14. Ensure that all laws related to TFV, including those addressing anonymity and encryption, respect human rights, including equality, privacy and freedom of expression. Any legal frameworks that impact those rights must be narrow, proportionate and justified. Broad, sweeping and generalized laws on these topics should be avoided.

15. Do not co-opt the vulnerability of equity-seeking groups to create overly broad government powers and protectionist laws that can unjustly infringe on human rights.

16. Provide adequate and appropriate training to all actors in the justice system — from police to judges — to ensure they have the skills and knowledge to properly address TFV using a human rights-based approach, including having the requisite knowledge on various technologies, digital evidence, human rights, racial bias, gender-based violence and discrimination against LGBTQ+ people.

17. Ensure that there are policies and legislation in place that adequately protect employees from discrimination and sexual harassment in the workplace. Ensure that there is particular attention paid to discrimination faced by employees in the technology sector.

18. Implement human rights-based content moderation regulation for internet intermediaries, including a requirement that companies publish transparency reports with anonymized disaggregated data on the types of violations and number of incidents faced by women, men, LGBTQ+ people and other equity-seeking groups, as well as the company's responses to them. These transparency reports should be published in ways that respect and protect the human rights, including privacy rights, of users.

19. Apply pressure to platforms to ensure user rights are respected and that those targeted with TFV on their platforms have accessible and understandable options regarding content removal, user suspension and other safety issues.

20. Implement privacy/data and consumer protection laws that require privacy by design and safety by design for technology companies and government actors creating or making use of digital technology.

21. Work collaboratively with the governments of other countries that are taking a human rights-based approach to addressing TFV. This could include cross-jurisdictional or international agreements that collectively address TFV and develop uniform human rights-based research, policies and legislation related to TFV.

22. Develop an international normative framework that outlines a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach to responding to TFV.

Funding and Resources

23. Provide adequate funding and resources to ensure that victims/survivors of TFV have a variety of options when seeking support, including legal and non-legal responses. These responses should allow victims/survivors time to consider their options. Responses should include accessible remedies that provide timely responses and do not require engagement with the legal system in all instances. Any support systems that are developed should take a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach to addressing TFV.

24. Ensure that there are independent and civil society organizations that are properly resourced to provide direct supports to victims/survivors of TFV. These organizations should be resourced to provide educational, social, technical, restorative and legal information about and supports around TFV that use a human rights-based approach. Support is particularly important for organizations that have expertise in supporting gender equality, LGBTQ+ rights, racial equality and other human rights. This could include developing resources such as independent helplines and civil society organizations where victims/survivors can get immediate psychosocial and technical support.

25. Support the development of independent government-funded bodies that employ a

human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach to provide public education and legal and non-legal supports for victims/survivors of TFV, including engaging with large tech companies to appropriately moderate content on their platforms. These bodies must be adequately resourced.

Research and Education

26. Provide resources to academic researchers and civil society organizations to conduct research on TFV, including collaborative research that engages relevant stakeholders. Funding allocations should ensure that equity-seeking groups and their interests are well represented in this research.

27. Collect disaggregated data on TFV to identify trends, especially the impact TFV has on equity-seeking groups, and to identify the effectiveness of the laws, policies and programs in place aimed at ending TFV. This data should include disaggregated information on who is targeted by and who is perpetrating TFV. Ensure that this data is collected and used in a manner that respects privacy, equality and other human rights.

28. Commit to supporting longitudinal research to assess the impacts of ongoing and new prevention and intervention programs, and the introduction or adaptation of laws and policies related to TFV.

29. Ensure that educational institutions, including elementary, secondary and post-secondary institutions, are educating people about TFV. This material should use a human rights-based approach and not be solely focused on privacy and safety information for potential victims/survivors. It should avoid an overly protectionist focus and should include information on respectful behaviour in digital spaces by all people. Education must focus on changing the behaviour of perpetrators and bystanders as well as protecting victims/survivors. Issues of technology should be integrated in healthy relationships and sexual education curricula.

30. Work in collaboration with civil society organizations and psychosocial support stakeholders to create and disseminate educational campaigns on TFV. Public education campaigns on TFV should assist victims/survivors of TFV, as well as address the harmful behaviour of perpetrators. Campaigns should avoid employing messages suggesting people not engage in digital spaces to avoid being harmed and not use victim-blaming language.

31. Work in collaboration with civil society organizations and academics when developing policies, regulations and education campaigns that address the root causes of many forms of TFV, including sexism, homophobia, transphobia, racism, ableism, religious discrimination and colonialism.

32. Education campaigns and programs should actively engage with men and boys about their role in creating and maintaining healthy digital spaces, including countering unhealthy behaviour in digital spaces.

33. Ensure that women and girls have equal access to the internet and digital technologies. Provide digital literacy education to women and girls to end the gendered digital divide.

34. Provide educational efforts and resources that encourage and support women and girls who wish to join the technology sector.

Technology Companies

Human Rights-Based Approach

1. Avoid business practices that prioritize content views and user engagement over ensuring platforms and products are compliant with human rights and safe for users.

2. Ensure that any algorithmic tools used do not amplify discriminatory content or discriminate against equity-seeking groups.

3. Ensure that their content moderation policies effectively address TFV using a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach, specifically TFV that impacts equity-seeking groups such as women, LGBTQ+ people, racial and ethnic minorities, disabled people and religious minorities.

Collaboration and Consultation

4. Meaningfully engage with civil society organizations, researchers and academics with expertise on TFV, as well as victims/survivors, to improve policies and responses to TFV.

5. Work collaboratively with civil society organizations that support victims/survivors of TFV to help facilitate fast-track channels related to serious incidents reported to those organizations.

Content Moderation and Technical Tools

6. Continue to develop and improve technical tools that users can use to protect themselves from TFV and provide clear information on how to use them. Provide adequate investment in these tools and education programs.

7. Ensure that content moderation policies are transparent and easy to use. Rules should be clear, and users should be able to determine what content is harmful according to those companies' policies. This should include clear appeal processes to challenge decisions.

8. Ensure that content moderation policies are accessible in the relevant language of their users.

9. Policies should use unambiguous language that clearly prohibits harmful content.

10. Using a human rights-based approach, ensure that content moderation policies are culturally specific and that content is evaluated within those contexts.

11. Content that breaches a company's content moderation policies should be removed reasonably swiftly to prevent the spread and repeated viewing of the content. Content that is particularly sensitive and harmful, such as child sexual abuse material and intimate images that have been shared without consent, should be prioritized to be removed as soon as possible.

12. Removal policies should not be discriminatory and should take a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach.

13. Ensure timely responses to complaints of TFV that violate content moderation rules, including appeals to decisions about the removal or non-removal of content. Responses must include clear explanations for why the decision was made.

14. Create dedicated flagging programs that fast-track cases. Publish a list of organizations that are a part of their trusted flagging programs. Provide information about how technology companies can join that program.

15. Ensure that digital evidence, including metadata, is retained by the company, and made available to the victim/survivor if required in a legal matter. The practices and reasonable timeline for maintaining data that could be used as evidence should be clearly stated in their policies.

16. Create and publish an audit of regionally relevant civil society organizations that provide supports and information on TFV. Provide financial and training resources to civil society organizations that provide this support and information, in particular in lower and middle-income regions.

Research and Education

17. Work collaboratively with civil society organizations and academics who conduct research on TFV prevention by providing access to relevant data that assists their research.

18. Provide accessible educational material to their users on digital safety and safe online practices, as well as information on how to navigate their content moderation practices.

19. Collect and publish transparency reports with disaggregated data on the types of violations and number of incidents faced by women, men, LGBTQ+ people and equity-seeking groups, as well as the responses to those violations, and routinely review the data to assess the effectiveness of policies and practices. Work collaboratively with civil society organizations and academics to review the data and determine best practices.

Equality and Safety in the Workplace

20. Employ human rights experts in TFV who can help develop technology and content moderation practices that best comply with human rights and safety standards.

21. Ensure that content moderation employees are adequately trained, earn a living wage and are provided relevant supports to manage the potential trauma related to viewing disturbing content as a part of their job.

22. Ensure that their workplaces are safe and welcoming to equity-seeking groups, including women, people of colour and LGBTQ+ people.

23. Diversify their workforce to ensure members of equity-seeking groups are represented and valued.

24. Ensure that their employees and developers are well trained about human rights, privacy and safety, including gender and sexual orientation discrimination.

25. Include privacy by design and safety by design practices in the development and implementation of their products and services.

Civil Society Organizations

Human Rights-Based Approach

1. Develop and expand on human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist research and supports.

Collaboration and Consultation

2. Work with governments and technology companies to develop policies, regulations and laws to address TFV.

3. Hold governments, technology companies and other stakeholders accountable for promises and actions to end TFV and mobilize actions where necessary.

4. Participate in global meetings with multilaterals and the private sector to push the agenda to end TFV and eliminate business models that benefit from or fail to address TFV.

5. Develop networks with other civil society organizations and academics to share research and support a global effort to end TFV.

Supports and Resources

6. Civil society organizations must be supported by governmental policies, legislation, regulation and resources to play a meaningful and central role in preventing TFV.

7. Engage with community members and victims/survivors to create culturally relevant resources and supports.

8. Provide social, technical, restorative and legal supports related to TFV that use a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist approach. This could include resources such as independent helplines, online services and in-person services where victims/survivors can get immediate psychosocial and technical supports.

9. Ensure staff have expertise in supporting women, LGBTQ+ people and other equity-seeking groups.

10. Develop human rights-based support networks and provisions for those who are impacted by TFV, in particular members of equity-seeking groups.

11. Do not require victims/survivors to engage with the justice system to access services.

12. Ensure services are confidential and victim centred.

Research and Education

13. Engage with community members and victims/survivors to create culturally relevant education campaigns and research aimed at preventing and responding to TFV.

14. Develop public education campaigns with a human rights focus aimed at preventing and addressing TFV, including the root causes of TFV (such as sexism, homophobia, transphobia,

racism, ableism, religious discrimination and colonialism).

15. Provide information on best practices for staying safe in digital spaces, and where to report and how best to manage incidents of TFV. This should include legal and non-legal options, including how to collect digital evidence needed in legal matters, how to report harmful content to technology companies as well as community-based responses to TFV.

Researchers, Academics and Think Tanks

Human Rights-Based Approach

1. Prioritize research agendas that examine the impact of TFV on equity-seeking groups, as well as the effectiveness of educational campaigns, policies, regulations, laws and supports available to victims/survivors of TFV.

2. Utilize a human rights-based, equity-focused, trauma-informed, survivor-centric and intersectional feminist framework when conducting research.

Collaboration and Consultation

3. Engage with the community that research is being conducted on and have them participate in and help guide the research whenever possible.

4. Work collaboratively with civil society organizations and governments at local, national, regional and international levels to address TFV.

5. Ensure research is presented in a way that can help influence political and regulatory decision making.

6. Participate in global meetings with multilaterals and the private sector to push the agenda to end TFV.

7. Develop hubs and collaborative spaces where academics, researchers, civil society organizations and governments can work together to share research, education and best practices to end TFV.

Research and Education

8. Further the research landscape on legal, regulatory, technical and social inputs to counter TFV and to monitor the status of TFV.

9. Conduct research on equity-seeking groups that are vulnerable to TFV, such as women, LGBTQ+ people, disabled people and members of marginalized racial, ethnic and religious groups.

10. Ensure research is conducted in relation to groups that may have smaller populations, but are greatly impacted by TFV, such as transgender people.

11. Conduct longitudinal research that can assess the long-term impact of TFV on victims and survivors, the effectiveness of policy changes, the impact of TFV prevention initiatives and curricula changes on prevalence rates of perpetration and victimization of TFV and attitudes toward TFV.

12. Conduct meta-analyses on TFV and its impacts that will provide strong evidence, which will encourage human rights-based policy changes.

13. Ensure knowledge mobilization within and beyond the academic community, including educational materials that are accessible to the population the research is relevant to.

Works Cited

7amleh — Arab Center for Social Media Advancement. 2018. "Online GBV in Palestine Means Losing Out on Women's Participation." GenderIt, June 11. www.genderit.org/feminist-talk/online-gbv-palestine-means-losing-out-womens-participation.

Abdullah, Mneera and Eliza Campbell. 2021. "Gendered violence online: cybersecurity for whom?" Middle East Institute, March 16. www.mei.edu/publications/gendered-violence-online-cybersecurity-whom.

Access Now. 2021. "10 facts to counter encryption myths." Access Now Policy Brief. August. www.accessnow.org/wp-content/uploads/2021/08/Encryption-Myths-Facts-Report.pdf.

Acoso. 2020. "Domestic violence and its online manifestations in the context of the pandemic." Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences. June.

Acosta, Rodrigo Vargas. 2020. "Regulatory issues in matters of freedom of expression and the internet in Latin America 2010–2020." Derechos Digitales. www.unesco.org/en/world-media-trends/regulatory-issues-matters-freedom-expression-and-internet-latin-america-2010-2020.

ADL Center for Technology and Society. 2021. *Online Hate and Harassment: The American Experience 2021*. March. www.adl.org/resources/report/online-hate-and-harassment-american-experience-2021.

African Declaration. 2015. "African Declaration on Internet Rights and Freedoms." https://africaninternetrights.org/en.

African Development Bank Group. 2016. "Minding the Gaps: Identifying Strategies to Address Gender-Based Cyber Violence in Kenya." Policy Brief. March. www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/Policy_Brief_on_Gender_Based_Cyber_Violence_in_Kenya.pdf.

Aghtaie, Nadia, Cath Larkins, Christine Barte, Nicky Stanley, Marsha Wood and Carolina Øverlien. 2018. "Interpersonal violence and abuse in young people's relationships in five European countries: online and offline normalisation of heteronormativity." *Journal of Gender-Based Violence* 2 (2): 293–310. https://doi.org/10.1332/239868018X15263879270302.

Aikenhead, Moira. 2021. "Revenge Pornography and Rape Culture in Canada's Nonconsensual Distribution Case Law." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn and Nicola Henry, 533–53. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211039.

Akbary, Artemis. 2022. "Afghan Queer Community's Access to the Internet Is a Double Edged Sword Under Taliban Rule." GenderIT, December 12. https://genderit.org/feminist-talk/afghan-queer-communitys-access-internet-double-edged-sword-under-taliban-rule.

Akter, Farhana. 2018. "Cyber Violence Against Women: The Case of Bangladesh." GenderIT, June 17. www.genderit.org/articles/cyber-violence-against-women-case-bangladesh.

Albury, Kath, Christopher Dietzel, Tinonee Pym, Son Vivienne and Teddy Cook. 2021. "Not your unicorn: trans dating app users' negotiations of personal safety and sexual health." *Health Sociology Review* 30 (1): 72–86. https://doi.org/10.1080/14461242.2020.1851610.

Alcaraz, María Florencia. 2017. "#NiUnaMenos: Politicising the Use of Technologies." GenderIT, September 4. https://genderit.org/feminist-talk/special-edition-niunamenos-politicising-use-technologies.

Amnesty International. 2018. "A Toxic Place for Women." In *#ToxicTwitter: Violence and Abuse against Women Online*. March 21. www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1-1/.

———. 2022. "South Korea: Online sexual abuse content proliferates as survivors blame Google failings." News, December 8. www.amnesty.org/en/latest/news/2022/12/south-korea-online-sexual-abuse-content-proliferates-as-survivors-blame-google-failings/.

Anasuya, Shreya Ila. 2018. "For Women in the Press Like Rana Ayyub, It's Scarily Easy for Online Threats to Turn Physical." GenderIT, June 7. www.genderit.org/feminist-talk/women-press-rana-ayyub-it%E2%80%99s-scarily-easy-online-threats-turn-physical.

Anderson, Briony and Mark A. Wood. 2021. "Doxxing: A Scoping Review and Typology." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn and Nicola Henry, 205–26. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211015.

Anwer, Zoya. 2022. "Navigating Identities: Experiencing Online Violence as a Shia Woman in Pakistan." GenderIT, October 29. https://genderit.org/feminist-talk/navigating-identities-experiencing-online-violence-shia-woman-pakistan.

APC & Humanist Institute for Cooperation with Developing Countries. 2013. *Global Information Society Watch 2013: Women's rights, gender and ICTs*. https://giswatch.org/sites/default/files/gisw13_chapters.pdf.

Arimatsu, Louise. 2019. "Silencing women in the digital age." *Cambridge International Law Journal* 8 (2): 187–217. https://doi.org/10.4337/cilj.2019.02.02.

Ashley, Florence. 2018a. "Don't be so hateful: The insufficiency of anti-discrimination and hate crime laws in improving trans well-being." *University of Toronto Law Journal* 68 (1): 1–36. https://doi.org/10.3138/utlj.2017-0057.

———. 2018b. "Genderfucking Non-Disclosure: Sexual Fraud, Transgender Bodies, and Messy Identities." *Dalhousie Law Journal* 41 (2): 339–77. https://digitalcommons.schulichlaw.dal.ca/dlj/vol41/iss2/3/.

Athar, Rima. 2015. "From Impunity to Justice: Improving Corporate Policies to End Technology-Related Violence Against Women." APC, February 25. www.apc.org/en/pubs/impunity-justice-improving-corporate-policies-end-0.

AWARE. 2020. "AWARE's Sexual Assault Care Centre saw 140 cases of technology-facilitated sexual violence in 2019, the most ever in one year." December 2. www.aware.org.sg/2020/12/awares-sexual-assault-care-centre-saw-140-cases-of-technology-facilitated-sexual-violence-in-2019-the-most-ever-in-one-year/.

Ayres França, Leandro and Jéssica Veleda Quevedo. 2020. "Project Leaked: Research on Non-Consensual sharing of Intimate Images in Brazil." *International Journal of Cyber Criminology* 14 (1): 1–28.

Aziz, Zarizana Abdul. 2020. *Online Violence Against Women in Asia: A Multicountry Study*. UN Women, November. www.aidsdatahub.org/sites/default/files/resource/unwomen-online-violence-against-women-asia-2020.pdf.

Badran, Mona Farid. 2019. "Bridging the gender digital divide in the Arab Region." IDRC. www.researchgate.net/publication/330041688_Bridging_the_gender_digital_divide_in_the_Arab_Region.

Baele, Stephane J., Lewys Brace and Travis G. Coan. 2019. "From 'Incel' to 'Saint': Analyzing the violent worldview behind the 2018 Toronto attack." *Terrorism and Political Violence* 33 (8): 1667–91. https://doi.org/10.1080/09546553.2019.1638256.

Bailey, Jane and Carissima Mathen. 2019. "Technology-Facilitated Violence against Women & Girls: Assessing the Canadian Criminal Law Response." *The Canadian Bar Review* 97 (3): 664–96. https://cbr.cba.org/index.php/cbr/article/view/4562.

Bailey, Jane and Suzie Dunn. Forthcoming 2023. "The More Things Change, The More They Stay the Same: Recurring Themes in Tech-facilitated Sexual Violence Over Time." In *Criminalising Intimate Image Abuse*, edited by Kolis Summerer and Gian Marco Calletti. Oxford, UK: Oxford University Press.

Bailey, Jane and Sara Shayan. 2016. "Missing and Murdered Indigenous Women Crisis: Technological Dimensions." *Canadian Journal of Women and the Law* 28 (2): 321–41. www.utpjournals.press/doi/abs/10.3138/cjwl.28.2.321.

Bailey, Jane, Nicola Henry and Asher Flynn. 2021. "Technology-Facilitated Violence and Abuse: International Perspectives and Experiences." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Nicola Henry and Asher Flynn, 1–17. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211001.

Bailey, Jane, Jacquelyn Burkell, Suzie Dunn, Chandell Gosse and Valerie Steeves. 2021. "AI and Technology-Facilitated Violence and Abuse." In *Artificial Intelligence and the Law in Canada*, edited by Florian Martin-Bariteau and Teresa Scassa. Toronto, ON: LexisNexis.

Bailey, Moya. 2021. *Misogynoir Transformed: Black Women's Digital Resistance*. New York, NY: New York University Press.

Barboni, Giorgia, Erica Field, Rohini Pande, Natalia Rigol, Simone Schaner and Charity Troyer Moore. 2018. *A Tough Call: Understanding barriers to and impacts of women's mobile phone adoption in India*. Harvard Kennedy School, October. www.hks.harvard.edu/publications/tough-call-understanding-barriers-and-impacts-womens-mobile-phone-adoption-india.

Barton, Alana and Hannah Storm. 2014. *Violence and Harassment against Women in the News Media: A Global Picture*. International Women's Media Foundation and International News Safety Institute. www.iwmf.org/wp-content/uploads/2018/06/Violence-and-Harassment-against-Women-in-the-News-Media.pdf.

Bartow, Ann. 2009. "Internet Defamation as Profit Center: The Monetization of Online Harassment." *Harvard Journal of Law and Gender* 32: 101–47.

Bauer, Greta R., Jake Pyne, Matt Caron Francino and Rebecca Hammond. 2013. "Suicidality among trans people in Ontario: Implications for social work and social justice." *Service Social* 59 (1): 35–62. https://doi.org/10.7202/1017478ar.

BC Society of Transition Houses. 2020. *Technology-Facilitated Violence: BC Anti-Violence Workers Survey Results Report.* February. https://bcsth.ca/wp-content/uploads/2021/03/16.-BCSTH-Tech_Facilitated-Violence-BC-Anti_Violence-Workers-Survey-Report-2020_Final.pdf.

Benjamini, Yoav and Yosef Hochberg. 1995. "Controlling the False Discovery Rate: A Practical and Powerful Approach to Multiple Testing." *Journal of the Royal Statistical Society*, Series B (Methodological) 57 (1): 289–300.

Bhandari, Vrinda and Anja Kovacs. 2021. "What's Sex Got to Do with It? Mapping the Impact of Questions of Gender and Sexuality on the Evolution of the Digital Rights Landscape in India." Internet Democracy Project, January 20. https://news.cyrilla.org/2021/01/new-report-whats-sex-got-to-do-with-it-mapping-the-impact-of-questions-of-gender-and-sexuality-on-the-evolution-of-the-digital-rights-landscape-in-india/.

Boyd, Susan B. and Elizabeth Sheehy. 2016. "Men's Groups: Challenging Feminism." *Canadian Journal of Women and the Law* 28 (1): 5–10. www.utpjournals.press/doi/abs/10.3138/cjwl.28.1.5?journalCode=cjwl.

Bradshaw, Samantha and Amélie Henle. 2021. "The Gender Dimensions of Foreign Influence Operations." *International Journal of Communication* (15): 4596–618.

Brandwatch. 2019. "Exposed: The Scale of Transphobia Online." www.brandwatch.com/reports/transphobia/.

Brown, Megan, Zeve Sanderson and Maria Alejandra Silva Ortega. 2022. "Gender-based online violence spikes after prominent media attacks." TechStream, Brookings Institute, January 26. www.brookings.edu/techstream/gender-based-online-violence-spikes-after-prominent-media-attacks/.

Burlock, Amanda and Tamara Hudon. 2018. "Women and men who experienced cyberstalking in Canada." Statistics Canada, June 5. www150.statcan.gc.ca/n1/pub/75-006-x/2018001/article/54973-eng.htm.

Canales, María Paz. 2017. "25N: Building an internet without violence." Derechos Digitales, November 24. www.derechosdigitales.org/11744/25n-construir-de-una-internet-sin-violencia/.

Center for Countering Digital Hate. 2022. "Hidden Hate: How Instagram fails to act on 9 in 10 reports of misogyny in DMs." https://counterhate.com/wp-content/uploads/2022/05/Final-Hidden-Hate.pdf.

Chair, Chenai, Ingrid Brudivg and Calum Cameron. 2020. "Women's Rights Online: Closing the digital gender gap for a more equal world." World Wide Web Foundation, October. https://webfoundation.org/research/womens-rights-online-2020/.

Chandrasekar, Ramya. 2017. *Policing online abuse or policing women? Our submission to the United Nations on online violence against women.* Internet Democracy Project, November 7. https://internetdemocracy.in/policy/un-srvaw-report.

Chisala-Tempelhoff, Sarai and Monica Twesiime Kirya. 2016. "Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda." *Palgrave Communications* 2 (1): 1–9. www.nature.com/articles/palcomms201669.

Citron, Danielle Keats. 2009. "Law's Expressive Value in Combating Cyber Gender Harassment." *Michigan Law Review* 108 (3): 373–476. https://repository.law.umich.edu/cgi/viewcontent.cgi?params=/context/mlr/article/1300/&path_info=.

———. 2014. *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press.

———. 2019. "Sexual Privacy." *The Yale Law Journal* 128 (7): 1870–1960.

———. 2022. *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. New York, NY: W. W. Norton.

Cole, Samantha. 2022. "The Legal System Is Completely Unprepared for Apple AirTag Stalking." Vice Motherboard, December 9. www.vice.com/en/article/5d3edx/apple-airtag-stalking-police-family-court.

Collins, Patricia Hill. 1990. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment.* London, UK: Routledge.

Conway, Maura, Ryan Scrivens and Logan Macnair. 2019. "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends." International Centre for Counter-Terrorism Policy Brief. November 25. https://icct.nl/app/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.

Coombs, Elizabeth. 2021. "Human Rights, Privacy Rights, and Technology-Facilitated Violence." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse,* edited by Jane Bailey, Asher Flynn and Nicola Henry, 475–91. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211036.

Council of Europe. 2018. "Mapping study on cyberviolence." T-CY(2017)10. July 9. Strasbourg, France: Council of Europe. https://rm.coe.int/t-cy-2017-10-cbgstudy-provisional/16808c4914.

Cox, Cassie. 2014. "Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosecutions and Effective Laws." *Jurimetrics* 54 (3): 277–302. www.jstor.org/stable/24395601.

Crenshaw, Kimberlé. 1991. "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color." *Stanford Law Review* 43 (6): 1241–99. https://doi.org/10.2307/1229039.

Crockett, Cailin and Rachel Vogelstein. 2022. "Launching the Global Partnership for Action on Gender-Based Online Harassment and Abuse." *Briefing Room* (White House Gender Policy Council blog), March 18. www.whitehouse.gov/gpc/briefing-room/2022/03/18/launching-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/.

Cuellar, Lina and Sandra Chaher. 2020. "Being a journalist on Twitter: Digital gender violence in Latin America." UNESCO.

Curlew, Abigail and Jeffery Monaghan. 2019. "Stalking 'Lolcows' and 'Ratkings': DIY Gender Policing, Far-Right Digilantes, and Anti-Transgender Violence." In *Disinformation and Digital Democracies in the 21st Century*, edited by Joseph McQuade, 24–28. Toronto, ON: NATO Association of Canada. https://natoassociation.ca/wp-content/uploads/2019/10/NATO-publication-.pdf.

Derechos Digitales. 2021. *Rapid Response Fund for the Protection of Digital Rights in Latin America: 2021 Milestones.* www.derechosdigitales.org/wp-content/uploads/Rapid-Response-Founf-2021-milestones.pdf.

DeKeseredy, Walter S. and Martin D. Schwartz. 2016. "Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory." *Sexualization, Media, & Society* 2 (4): 1–8. https://doi.org/10.1177/2374623816684692.

Devika, J. 2019. "Gender-Based Cyber Violence against Women in Kerala: Insights from Recent Research." Centre for Development Studies. https://cds.edu/wp-content/uploads/2021/02/7Commentary-min.pdf.

Dhrodia, Azmina. 2018. "Unsocial media: A toxic place for women." *IPPR Progressive Review* 24 (4): 380–87. https://doi.org/10.1111/newe.12078.

Díaz, Marianne and Jamila Venturini. 2020. "Identity systems and social protection in Venezuela and Bolivia: gender impacts and other inequalities." Derechos Digitales. www.derechosdigitales.org/wp-content/uploads/identity-systems_ENG.pdf.

Dietzel, Christopher. 2021. "'That's Straight-Up Rape Culture': Manifestations of Rape Culture on Grindr." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn and Nicola Henry, 351–68. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211026.

———. 2022. "The three dimensions of unsolicited dick pics: Sexual minority men's experiences of sSending and receiving unsolicited dick pics on dating apps." *Sexuality & Culture* (26): 834–52.

Digital Rights Foundation. 2017a. *Measuring Pakistani Women's Experiences of Online Violence: A Quantitative Research Study on Online-Gender Based Harassment in Pakistan.* https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

———. 2017b. "Surveillance of Female Journalists in Pakistan." https://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female-Journalists-in-Pakistan-1.pdf.

———. 2019. "Female Journalists in New Media: Experiences, challenges and a gendered approach." https://digitalrightsfoundation.pk/wp-content/uploads/2019/03/Female-journalists-in-new-media-experiences-challenges-and-a-gendered-approach.pdf.

Dodge, Alexa. 2021. *Deleting Digital Harm: A Review of Nova Scotia's CyberScan Unit.* August. Halifax, NS: Dalhousie University. www.vawlearningnetwork.ca/docs/CyberScan-Report.pdf.

Dodge, Alexa, Dale Spencer, Rose Ricciardelli and Dale Ballucci. 2019. "'This isn't your father's police force': Digital evidence in sexual assault investigations." *Journal of Criminology* 52 (4): 499–515. https://doi.org/10.1177/0004865819851544.

Douglas, Heather, Bridget A. Harris and Molly Dragiewicz. 2019. "Technology-facilitated Domestic and Family Violence: Women's Experiences." *The British Journal of Criminology* 59 (3): 551–70.

Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock and Bridget Harris. 2018. "Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms." *Feminist Media Studies* 18 (4): 1–17. https://doi.org/10.1080/14680777.2018.1447341.

Duggan, Maeve. 2017. *Online Harassment 2017*. Pew Research Center. July 11. www.pewresearch.org/internet/2017/07/11/online-harassment-2017/.

Dunn, Suzie. 2020a. *Technology-Facilitated Gender-Based Violence: An Overview*. Supporting a Safer Internet Paper No. 1. Waterloo, ON: CIGI. www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/.

———. 2020b. "Identity Manipulation: Responding to Advances in Artificial Intelligence and Robotics." We Robot 2020 Conference Paper.

Dunn, Suzie and Moira Aikenhead. 2022. "On the Internet, Nobody Knows You are a Dog: Contested Authorship of Digital Evidence in Cases of Gender-based Violence." *Canadian Journal of Law and Technology* 19 (2): 371–409.

Dunn, Suzie and Alessia Petricone-Westwood. 2018. "More than 'Revenge Porn' Civil Remedies for the Nonconsensual Distribution of Intimate Images." 38th Annual Civil Litigation Conference.

Eaton, Asia A., Divya Ramjee and Jessica F. Saunders. 2022. "The Relationship between Sextortion during COVID-19 and Pre-pandemic Intimate Partner Violence: A Large Study of Victimization among Diverse U.S. Men and Women." *Victims & Offenders* 18 (2): 338–55. www.tandfonline.com/doi/bs/10.1080/15564886.2021.2022057?journalCode=uvao20.

Eckert, Stine and Jade Metzger-Riftkin. 2020. "Doxxing, privacy and gendered harassment: The Shock and Normalization of Veillance Cultures." APC, August 10. www.apc.org/en/press/doxxing-privacy-and-gendered-harassment-shock-and-normalization-veillance-cultures.

El Heraldo. 2020. "Feministas denuncian que filtración de fotos íntimas aumentó en cuarentena." *El Heraldo*, April 25. www.heraldo.mx/feministas-denuncian-que-filtracion-de-fotos-intimas-aumento-en-cuarentena/.

eSafety Commissioner. 2019. *eSafety for Women from Culturally and Linguistically Diverse Backgrounds*. February. www.esafety.gov.au/sites/default/files/2019-07/summary-report-for-women-from-cald-backgrounds.pdf.

———. 2021. *Protecting LGBTIQ+ voices online: resource development research*. August. www.esafety.gov.au/research/protecting-lgbtiq-voices-online.

European Institute for Gender Equality. 2017. "Cyber violence against women and girls." https://eige.europa.eu/publications/cyber-violence-against-women-and-girls.

———. 2019. *Gender equality and youth: opportunities and risks of digitalisation*. https://eige.europa.eu/publications/gender-equalityand-youth-opportunities-andrisks-digitalisation.

———. 2022. *Combating Cyber Violence against Women and Girls*. https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls.

Fairbairn, Jordan. 2015. "Rape threats and revenge porn: Defining sexual violence in the digital age." In *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices,* edited by Jane Bailey and Valerie Steeves. Ottawa, ON: University of Ottawa Press.

Farokhmanesh, Megan. 2022. "The End of Kiwi Farms, the Web's Most Notorious Stalker Site." Wired, September 8. www.wired.com/story/keffals-kiwifarms-cloudflare-blocked-clara-sorrenti/.

Farrell, Andrew. 2021. "It's Just a Preference: Indigenous LGBTIQ+ Peoples and Technologically Facilitated Violence." In *The Palgrave Handbook of Gendered Violence and Technology,* edited by Anastasia Powell, Asher Flynn and Lisa Sugiura, 335–53. Cham, Switzerland: Palgrave Macmillan.

Fascendini, Flavia. 2014. "Highlights on Tech-Related Violence Against Women in Bosnia and Herzegovina, Mexico and the Philippines." GenderIT, December 12. https://genderit.org/feminist-talk/highlights-tech-related-violence-against-women-bosnia-and-herzegovina-mexico-and.

Fascendini, Flavia and Kateřina Fialová. 2011. *Voices from digital spaces: Technology related violence against women*. APC. December. www.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdfwww.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf.

Ferrier, Michelle. 2018. *Attacks and Harassment: The Impact of Female Journalists and Their Reporting*. TrollBusters and International Women's Media Foundation.

FRA — European Union Agency for Fundamental Rights. 2014. *Violence against women: an EU-wide survey*. http://fra.europa.eu/en/publication/2014/violence-against-women-eu-widesurvey-main-results-report.

France 24. 2021. "Hackers release Israeli LGBTQ dating site details." November 2. www.france24.com/en/live-news/20211102-hackers-release-israeli-lgbtq-dating-site-details.

Franks, Mary Anne. 2015. "Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators." https://ssrn.com/abstract=2468823.

Freed, Diana, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart and Nicola Dell. 2018. "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology." CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3173574.3174241.

GenderIT. 2015. "End Violence: Case Studies from Mexico." GenderIT, February 15. https://genderit.org/resources/end-violence-case-studies-mexico.

———. 2018a. "We Can Be Heroes: Towards Public and Legal Recognition of Online Gender-Based Violence." GenderIT, June 17. www.genderit.org/edition/we-can-be-heroes-towards-public-and-legal-recognition-online-gender-based-violence.

———. 2018b. "13 Manifestations of Gender-Based Violence Using Technology." GenderIT, November 12. https://genderit.org/resources/13-manifestations-gender-based-violence-using-technology.

Ghoshal, Neela. 2020. *"Every Day I Live in Fear": Violence and Discrimination Against LGBT People in El Salvador, Guatemala, and Honduras, and Obstacles to Asylum in the United States.* Human Rights Watch, October 7. www.hrw.org/report/2020/10/07/every-day-i-live-fear/violence-and-discrimination-against-lgbt-people-el-salvador.

Gill, Lex, Tamir Israel and Christopher Parsons. 2018. *Shining a Light on the Encryption Debate: A Canadian Field Guide.* The Citizen Lab and the Canadian Internet Policy & Public Interest Clinic. May. https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.

Gillwald, Alison. 2018. *Understanding the Gender Gap in the Global South.* After Access. https://afteraccess.net/wp-content/uploads/2018-After-Access-Understanding-the-gender-gap-in-the-Global-South.pdf.

GLAAD. 2022. "Unsafe in America: New GLAAD Data Shows Unprecedented Threats and Attacks Against LGBTQ Americans Leading Up to the Deadly Mass Shooting in Colorado Springs." News release, November 22. www.glaad.org/releases/unsafe-america%C2%A0-new-glaad-data-shows-unprecedented-threats-and-attacks-against-lgbtq.

Global Information Society Watch. 2017. *Unshackling Expression: A Study on Laws Criminalising Expression Online in Asia.* https://giswatch.org/2017-special-report-unshackling-expression-study-law-criminalising-expression-online-asia.

Global Partnership for Action on Gender-Based Online Harassment and Abuse. Forthcoming 2023. *Technology-Facilitated Gender-Based Violence Evidence Situation Report.*

Goldberg, Carrie. 2019. *Nobody's Victim: Fighting Psychos, Stalkers, Pervs, and Trolls.* New York, NY: Plume.

Goulds, Sharon, Miriam Gauer, Aisling Corr and Jacqui Gallinetti. 2020. *Free to Be Online? Girls' and young women's experiences of online harassment.* Plan International. https://plan-international.org/publications/free-to-be-online/.

Green, Yasmin. 2022. "Iran's Internet Blackouts Are Part of a Global Menace." *Wired,* October 19. www.wired.com/story/iran-mahsa-amini-internet-shutdown/.

Gritten, David. 2022. "Iran sentences two LGBT activists to death." BBC News, September 6. www.bbc.com/news/world-middle-east-62793573.

GSMA and Cherie Blair Foundation for Women. 2013. *Women & Mobile: A Global Opportunity. A study on the mobile phone gender gap in low and middle-income countries.* www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/GSMA_Women_and_Mobile-A_Global_Opportunity.pdf.

Guerra, Juliana and Mallory Knodel. 2019. "Feminism and protocols." Internet Engineering Task Force, July 8.

Gurumurthy, Anita and Amrita Vasudevan. 2018. "Hidden Figures: A Look at Technology-Mediated Violence against Women in India." Gender IT, June 11. www.genderit.org/articles/hidden-figures-look-technology-mediated-violence-against-women-india.

Gurumurthy, Anita and Amshuman Dasarathy. 2022. *Profitable Provocations A Study of Abuse and Misogynistic Trolling on Twitter Directed at Indian Women in Public-political Life.* IT for Change, July. https://itforchange.net/sites/default/files/2132/ITfC-Twitter-Report-Profitable-Provocations.pdf.

Guy, Rachel. 2021. "Nation of Men: Diagnosing Manospheric Misogyny as Virulent Online Nationalism." *Georgetown Journal of Gender and the Law* 22 (3): 601–40. https-//ssrn.com/abstract=3939252.

Hall, Matthew and Jeff Hearn. 2019. "Revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts." *Journal of Gender Studies* 28 (2): 158–70.

Hassan, Bushra, Tim Unwin and Akber Gardezi. 2018. "Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan." *Information Technologies & International Development* 14: 1–17.

Hassan, Fatma Mohammed, Fatma Nada Khalifa, Eman D. El Desouky, Marwa Rashad Salem and Mona Mohamed Ali. 2020. "Cyber violence pattern and related factors: online survey of females in Egypt." *Egyptian Journal of Forensic Sciences* 10 (6): 1–7. https://ejfs.springeropen.com/articles/10.1186/s41935-020-0180-0.

Hasinoff, Amy Adele. 2014. "Blaming Sexualizaton for Sexting." *Girlhood Studies* 7 (1): 102–20.

Havron, Sam, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell and Thomas Ristenpart. 2019. "Clinical Computer Security for Victims of Intimate Partner Violence." 28th USENIX Security Symposium. www.usenix.org/conference/usenixsecurity19/presentation/havron.

Hayes, Rebecca M. and Molly Dragiewicz. 2018. "Unsolicited dick pics: Erotica, exhibitionism or entitlement?" *Women's Studies International Forum* 71: 114–20.

Hébert, William, Nora Butler Burke, Tara Santini, Frank Suerich-Gulick and Daphne Barile. 2022. *A Qualitative Look at Serious Legal Problems: Trans, Two-Spirit, and Non-Binary People in Canada*. Department of Justice Canada.

Henry, Nicola and Asher Flynn. 2019. "Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support." *Violence Against Women* 25 (16): 193–95. https://doi.org/10.1177/1077801219863881.

Henry, Nicola, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell and Adrian J. Scott. 2020. *Image-based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery*. New York, NY: Routledge.

Hernández Bauzá, Valentina. 2017. *Technology for Privacy and Freedom of Expression: Regulation of Anonymity and Encryption*. Derechos Digitales. www.derechosdigitales.org/wp-content/uploads/anonimity-and-encryption.pdf.

———. 2020. "Trends related to regulatory developments in privacy and the internet in Latin America." Derechos Digitales, January 1.

Hinson, L., L. O'Brien-Milne, J. Mueller, V. Bansal, N. Wandera and S. Bankar. 2019. "Defining and Measuring Technology-Facilitated Gender-Based Violence." International Center for Research on Women. www.icrw.org/wp-content/uploads/2019/03/ICRW_TFGBVMarketing_Brief_v4_WebReady.pdf.

Horwitz, Jeff. 2021. "Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt." *The Wall Street Journal*, September 13. www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353.

Hrick, Pam. 2021. "The Potential of Centralized and Statutorily Empowered Bodies to Advance a Survivor-Centered Approach to Technology-Facilitated Violence Against Women." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn and Nicola Henry, 595–615. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211043.

Hsu, Jason C. 1996. *Multiple Comparisons: Theory and methods*. London, UK: Chapman & Hall/CRC Press.

Hupfer, Susanne, Sayantani Mazumder, Ariane Bucaille and Gillian Crossan. 2021. "Women in the tech industry: Gaining ground, but facing new headwinds." Deloitte, December 1. www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2022/statistics-show-women-in-technology-are-facing-new-headwinds.html.

Human Rights Watch. 2019. "'Don't Punish Me for Who I Am': Systemic Discrimination Against Transgender Women in Lebanon." September 3. www.hrw.org/report/2019/09/03/dont-punish-me-who-i-am/systemic-discrimination-against-transgender-women-lebanon.

———. 2020. "Egypt: Security Forces Abuse, Torture LGBT People." October 1. www.hrw.org/news/2020/10/01/egypt-security-forces-abuse-torture-lgbt-people.

Inter-Parliamentary Union. 2016. "Sexism, harassment and violence against women parliamentarians." Issues Brief. October. www.iknowpolitics.org/en/learn/knowledge-resources/report-white-paper/ipu-issues-brief-sexism-harassment-and-violence-against.

International Federation of Journalists. 2017. "IFJ survey: One in two women journalists suffer gender-based violence at work." November 24.

Internet Sans Frontières. 2019. "#IWD2019: Online Gender-Based Violence Affects 45% of Women on Social Media in West and Central Africa." https://internetwithoutborders.org/iwd2019-online-gender-based-violence-affects-45-of-women-on-social-media-in-west-and-central-africa/

ITU. 2022. *Measuring digital development: Facts and Figures 2022*. www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

Iyer, Neema, Bonnita Nyamwire and Sandra Nabulega. 2020. *Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet*. APC. August. www.apc.org/en/pubs/alternate-realities-alternate-internets-african-feminist-research-feminist-internet.

Iyer, Neema, Garnett Achieng, Favour Borokini and Uri Ludger. 2021. *Automated Imperialism, Expansionist Dreams: Exploring Digital Extractivism in Africa*. Pollicy. June. https://archive.pollicy.org/wp-content/uploads/2021/06/Automated-Imperialism-Expansionist-Dreams-Exploring-Digital-Extractivism-in-Africa.pdf.

Jain, Tripti. 2021. "Tech Tools to Facilitate and Manage Consent: Panacea or Predicament? A Feminist Perspective." Data Governance Network Working Paper 21. Internet Democracy Project, January 10. https://internetdemocracy.in/reports/tech-tools-to-facilitate-and-manage-consent.

James, Sandy, Jody Herman, Susan Rankin, Mara Keisling, Lisa Mottet and Ma'ayan Anafi. 2016. *The Report of the 2015 U.S. Transgender Survey*. Washington, DC: National Center for Transgender Equality. December. https://transequality.org/sites/default/files/docs/usts/USTS-Full-Report-Dec17.pdf.

Jamil, Sadia. 2021. "From digital divide to digital inclusion: Challenges for wide-ranging digitalization in Pakistan." *Telecommunications Policy* 45 (8): 102206. https://doi.org/10.1016/j.telpol.2021.102206.

Jane, Emma. 2018. "Gendered cyberhate as workplace harassment and economic vandalism." *Feminist Media Studies* 18 (4): 575–91. https://doi.org/10.1080/14680777.2018.1447344.

Jankowicz, Nina, Jillian Hunchak, Alexandra Pavliuc, Celia Davies, Shannon Pierson and Zoë Kaufmann. 2021. *Malign Creativity: How Gender, Sex, and Lies Are Weaponized against Women Online*. Washington, DC: Wilson Center. www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online.

Jansen Reventlow, Nani. 2017. "Online harassment of women journalists and iInternational law: not 'just' a gender issue, but a threat to democracy." Berkman Klein Center Collection, November 16.

Judson, Ellen. 2021. "Gendered disinformation: 6 reasons why liberal democracies need to respond to this threat." Demos, July. https://demos.co.uk/blog/gendered-disinformation/.

Judson, Ellen, Asli Atay, Alex Krasodomski-Jones, Rose Lasko-Skinner and Josh Smith. 2020. *Engendering Hate: The contours of state-aligned gendered disinformation online*. Demos, October 26. https://demos.co.uk/project/engendering-hate-the-contours-of-state-aligned-gendered-disinformation-online/.

Kamran, Hija and Meher Ahmad. 2021. "Pakistan's revenge porn law is stronger than most. For one woman, that made no difference." Rest of World, April 30. https://restofworld.org/2021/pakistans-revenge-porn-law-is-stronger-than-most-for-one-woman-that-made-no-difference/.

Kapiyo, Victor. 2022. "Bridging the Gender Digital Divide is Critical for Achieving Digital Rights in Africa." Collaboration on International ICT Policy for East and Southern Africa, June 30. https://cipesa.org/2022/06/bridging-the-gender-digital-divide-is-critical-for-achieving-digital-rights-in-africa/.

Karaian, Lara. 2012. "Lolita speaks: 'Sexting,' teenage girls and the law." *Crime Media Culture* 8 (1): 57–73.

———. 2013. "Policing 'sexting': Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers' digital sexual expression." *Theoretical Criminology* 18 (3): 282–99. https://doi.org/10.1177/1362480613504331.

Kaul, Nitasha. 2021. "The Misogyny of Authoritarians in Contemporary Democracies." *International Studies Review* 23 (4): 1619–45. https://doi.org/10.1093/isr/viab028.

Kayastha, Shubha and Rita Baramu. 2021. *Mapping Laws Relevant to Online Violence in Nepal*. Body & Data. https://bodyanddata.org/wp-content/uploads/2021/12/OnlineGBVLawsMapping-min.pdf.

Kee, Jac sm. 2005. "Cultivating Violence Through Technology? Exploring the Connections between Information Communication Technologies (ICT) and Violence Against Women (VAW)." APC, April 16. https://genderit.org/es/node/1813.

Kee, Jac sm and Sonia Randhawa. 2010. "Malaysia: Violence against Women and Information Communication Technologies." GenderIT, June 1. https://genderit.org/resources/malaysia-violence-against-women-and-information-communication-technologies.

Khan, Irene. 2021. *#JournalistsToo: Women Journalists Speak Out*. UNESCO and United Nations Human Rights Special Procedures. https://srfreedex.org/journalists-too/.

Khoo, Cynthia. 2021. *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence*. Toronto, ON: LEAF. www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf.

Khoo, Cynthia, Kate Robertson and Ronald Deibert. 2019. *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*. The Citizen Lab, June 12. https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/.

Kirchgaessner, Stephanie. 2022. "Two female activists in Bahrain and Jordan hacked with NSO spyware." *The Guardian*, January 17. www.theguardian.com/news/2022/jan/17/two-female-activists-in-bahrain-and-jordan-hacked-with-nso-spyware.

Klein, Jessica and Kristen Zaleski. 2019. "Non-Consensual Image Sharing-Revenge Pornography and Acts of Sexual Assault Online." In *Women's Journey to Empowerment in the 21st Century: A Transnational Feminist Analysis of Women's Lives in Modern Times*, edited by Kristen Zaleski, Annalisa Enrile, Eugenia L. Weiss and Xiying Wang. New York, NY: Oxford University Press.

Kovacs, Anja. 2017. "'Chupke, Chupke': Going Behind the Mobile Phone Bans in North India." Gendering Surveillance. Internet Democracy Project, February. https://genderingsurveillance.internetdemocracy.in/phone_ban/.

Kovacs, Anja and Tripti Jain. 2021. "Informed consent — Said who? A feminist perspective on principles of consent in the age of embodied data — A policy brief." Internet Democracy Project, March 22. https://internetdemocracy.in/policy/informed-consent-said-who-a-feminist-perspective-on-principles-of-consent-in-the-age-of-embodied-data-a-policy-brief.

Kovacs, Anja, Richa Kaul Padte and Shobha SV. 2013. "*Don't Let It Stand": An Exploratory Study of Women and Verbal Online Abuse in India*. Internet Democracy Project. April. https://internetdemocracy.in/reports/women-and-verbal-online-abuse-in-india.

Kovacs, Anja, Avri Doria, Bruno Zilli, Margarita Salas and Women's Legal and Human Rights Bureau. 2012. *Critically Absent: Women in Internet Governance*. APC. April 3. www.apc.org/en/pubs/critically-absent-women-internet-governance-policy.

Kraicer, Eve. 2020. "Online and ICT facilitated violence against women and girls during COVID-19." UN Women. www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19.

Kraicer, Eve and Azmina Dhrodia. 2021. "'Women shouldn't be expected to pay this cost just to participate.' Online Gender-Based Violence and Abuse: Consultation Briefing." World Wide Web Foundation, October 6. https://webfoundation.org/research/women-shouldnt-be-expected-to-pay-this-cost-just-to-participate-online-gender-based-violence-and-abuse-consultation-briefing/.

Kuroda, Reiko, Mariana Lopez, Janelle Sasaki and Michelle Settecase. 2019. "The Digital Gender Gap." www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Equity-Policy-Brief-W20-Japan.pdf.

La Prensa. 2020. "Redes sociales, el espacio que han encontrado las mujeres nicaragüenses para denunciar a sus agresores." April 14. www.laprensa.com.ni/2020/04/14/nacionales/2662961-redes-sociales-el-espacio-que-han-encontrado-las-mujeres-nicaraguenses-para-denunciar-a-sus-agresores.

Lenhart, Amanda, Michele Ybarra and Myeshia Price-Feeney. 2016. "Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of 'Revenge Porn.'" Data & Society Research Institute. December 13. https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf.

Lenhart, Amanda, Michele Ybarra, Kathryn Zickuhr and Myeshia Price-Feeney. 2016. "Online Harassment, Digital Abuse, and Cyberstalking in America." Data & Society Research Institute. November 21. www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

Levy, Karen and Bruce Schneier. 2020. "Privacy threats in intimate relationships." *Journal of Cybersecurity* 6 (1): 1–13. https://doi.org/10.1093/cybsec/tyaa006.

Lirri, Evelyn. 2015. "The Challenge of Tackling Online Violence Against Women in Africa." *Collaboration on International ICT Policy for East and Southern Africa Blog*, October 2. https://cipesa.org/2015/10/the-challenge-of-tackling-online-violence-against-women-in-africa/.

Lo, Madison. 2021. "A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies Under Current Law." *California Law Review* (109): 277–315. https://doi.org/10.15779/Z38XW47X1J.

Lodhi, Annam. 2018. "Women Journalists & the Double Bind: Choosing silence over being silenced." Media Matters for Democracy, July 18. www.apc.org/en/pubs/women-journalists-and-double-bind-choosing-silence-over-being-silenced.

Lokot, Tetyana. 2018. "#IAmNotAfraidToSayIt: stories of sexual violence as everyday political speech on Facebook." *Information, Communication & Society* 21 (6): 802–17. https://doi.org/10.1080/1369118X.2018.1430161.

Lopes Gomes Pinto Ferreira, Gisella. 2021. "Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence: Perspectives from Advocates in the Global-South." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn and Nicola Henry, 427–46. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211032/full/html.

Louie, Yee Man. 2021. "Technology-Facilitated Domestic Abuse and Culturally and Linguistically Diverse Women in Victoria, Australia." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn and Nicola Henry, 447–67. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211033.

Lui, Michelle, Brittany Singh and Giovanni Giuga. Forthcoming 2023. "Pro-Pronouns: Gender Identities on Social Media, Video Conferencing, and Learning Platforms." In *Can't Compute*. Ottawa, ON: University of Ottawa Research Chair in Technology and Society. www.cantcompute.ca/.

Machirori, Fungai. 2017. "Towards a gender-just internet: Combating online violence against women." Africa Portal, September 29. www.africaportal.org/features/gender-just-internet-how-do-we-combat-online-violence/.

Mahmutović, Aida, hvale vale and Vasilika Laçí. 2021. *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach*. Geneva, Switzerland: Geneva Centre for Security Sector Governance.

Makinde, Olusesan Ayodeji, Emmanuel Olamijuwon, Nchelem Kokomma Ichegbo, Cheluchi Onyemelukwe and Michael Gboyega Ilesanmi. 2021. "The Nature of Technology-Facilitated Violence and Abuse among Young Adults in Sub-Saharan Africa." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn and Nicola Henry, 83–101. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211005.

Malanga, Donald Flywell. 2020. "Tackling gender-based cyber violence against women and girls in Malawi amidst the COVID-19 pandemic." African Internet Rights. https://africaninternetrights.org/sites/default/files/Donald_Flywell.pdf.

———. 2021. "Survey of Cyber Violence against Women in Malawi." Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development. https://arxiv.org/ftp/arxiv/papers/2108/2108.09806.pdf.

Manjoo, Rashida. 2012. "The Continuum of Violence against Women and the Challenges of Effective Redress." *International Human Rights Law Review* 1 (1): 1–29. https://doi.org/10.1163/22131035-00101008.

Marwick, Alice E. 2017. "Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks." *Ethics and Information Technology*, 19 (3): 177–91. https://doi.org/10.1007/s10676-017-9431-7.

Marwick, Alice E. and Robyn Caplan. 2018. "Drinking male tears: language, the manosphere, and networked harassment." *Feminist Media Studies* 18 (4): 543–59. https://doi.org/10.1080/14680777.2018.1450568.

Massanari, Adrienne L. 2018. "Rethinking Research Ethics, Power, and the Risk of Visibility in the Era of the 'Alt-Right' Gaze." *Social Media & Society* 2 (4): 1–9. https://journals.sagepub.com/doi/10.1177/2056305118768302.

Maurya, Chanda, T. Muhammad, Preeti Dhillon and Priya Maurya. 2022. "The effects of cyberbullying victimization on depression and suicidal ideation among adolescents and young adults: a three year cohort study from India." *BMC Psychiatry* 22 (599). https://doi.org/10.1186/s12888-022-04238-x.

McCulloch, Jude, Sandra Walklate, JaneMaree Maher, Kate Fitz-Gibbon and Jasmine McGowan. 2019. "Lone Wolf Terrorism Through a Gendered Lens: Men Turning Violent or Violent Men Behaving Violently?" *Critical Criminology* 27: 437–50. https://doi.org/10.1007/s10612-019-09457-5.

McGinley, Ann C. 2022. "Misogyny and Murder." *Harvard Journal of Law & Gender* 45: 177– 247. http://harvardjlg.com/wp-content/uploads/sites/19/2022/09/Misogyny-and-Murder.pdf.

McGlynn, Clare. n.d. "Korean Lessons on Supporting Victims of Image-Based Abuse." https://claremcglynn.com/imagebasedsexualabuse/korean-lessons-on-supporting-victims-of-image-based-sexual-abuse/.

———. 2016. "Anonymity for Complainants of Image-Based Sexual Abuse: focus on harms to victims, not motives of perpetrators." Centre for Gender Equal Media. https://claremcglynn.files.wordpress.com/2016/07/mcglynn-anonymity-revenge-porn-11-july-2016.pdf.

McGlynn, Clare and Erika Rackley. 2017. "Image-Based Sexual Abuse." *Oxford Journal of Legal Studies* 37 (3): 534–61. https://doi.org/10.1093/ojls/gqw033.

McGlynn, Clare and Kelly Johnson. 2021. *Cyberflashing: Recognising Harms, Reforming Laws*. Bristol, UK: Bristol University Press.

McMahon, Rob, Tim LaHache and Tim Whiteduck. 2015. "Digital Data Management as Indigenous Resurgence in Kahnawà:ke." *International Indigenous Policy* Journal 6 (3): 1–19. https://doi.org/10.18584/iipj.2015.6.3.6.

Media Foundation for West Africa. 2017. *Women's Rights Online: Issues in Ghana*. www.mfwa.org/wp-content/uploads/2018/02/Baseline-Report-WRO-Issues-in-Ghana.pdf.

Mehta, Ivan. 2022. "Twitter disperses the Trust & Safety Council after key members resigned." Tech Crunch, December 12. https://techcrunch.com/2022/12/12/twitter-disperses-the-trust-safety-council-after-key-members-resigned/.

Miles, Katrina. 2020. "The law on underage sexting needs to change — here's how." The Conversation, March 4. https://theconversation.com/the-law-on-underage-sexting-needs-to-change-heres-how-132473.

Milmo, Dan. "Elon Musk reinstates Donald Trump's Twitter account after taking a poll." *The Guardian*, November 20. www.theguardian.com/us-news/2022/nov/20/twitter-lifts-donald-trump-ban-after-elon-musks-poll.

Moloney, Anastasia. 2019. "LGBT+ murders at 'alarming' levels in Latin America — study." Reuters, August 8. www.reuters.com/article/us-latam-lgbt-killings-idUSKCN1UY2GM.

Moolman, Jan. 2018. "Recognition of Online GBV in International Law: The Highs and Lows." APC, June 17. www.genderit.org/editorial/editorial-recognition-online-gbv-international-law-highs-and-lows.

Munusamy, Kiruba. 2018. "Intersection of Identities: Online Gender and Caste Based Violence." GenderIT, June 7. www.genderit.org/articles/intersection-identities-online-gender-and-caste-based-violence.

Muya, Catherine. 2021. "The Law Should Work for Us: Assessing Gaps in Kenya's Regulatory Framework to Build a Safer Internet for Women and Girls." Open Internet for Democracy Initiative. https://openinternet.global/sites/default/files/2021-09/The%20Law%20Should%20Work%20for%20Us.pdf.

Namaste, Ki. 1996. "Genderbashing: Sexuality, Gender, and the Regulation of Public Space." *Environment and Planning D: Society and Space* 14 (2): 221–40. https://doi.org/10.1068/d140221.

National Coalition of Anti-Violence Programs. 2016. *Lesbian, Gay, Bisexual, Transgender, Queer, and HIV-Affected Intimate Partner Violence in 2015*. New York, NY: National Coalition of Anti-Violence Programs. https://avp.org/wp-content/uploads/2017/04/2015_ncavp_lgbtqipvreport.pdf.

National Network to End Domestic Violence. 2014. "A Glimpse from the Field: How Abusers Are Misusing Technology." https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/54e3d1b6e4b08500fcb455a0/1424216502058/NNEDV_Glimpse+From+the+Field+-+2014.pdf.

Neris, Natália, Juliana Pacetta Ruiz and Mariana Giorgetti Valente. 2018. "Fighting the Dissemination of Non-Consensual Intimate Images: a comparative analysis." Internet Lab. www.internetlab.org.br/wp-content/uploads/2018/11/Fighting_the_Dissemination_of_Non.pdf.

Nguyen, Erica and Heather Barr. 2020. "Thinking beyond punishment to combat digital sex crimes." *The Korea Times*, May 20. www.koreatimes.co.kr/www/opinion/2020/05/197_289806.html.

Nova, Fayika Farhat, Md. Rashidujjaman Rifat, Pratyasha Saha, Syed Ishtiaque Ahmed and Shion Guha. 2019. "Online sexual harassment over anonymous social media in Bangladesh." *ICTD '19: Proceedings of the Tenth International Conference on Information and Communication Technologies and Development*. https://doi.org/10.1145/3287098.3287107.

Nwaodike, Chioma and Nerissa Naidoo. 2020. *Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks in Ethiopia, Kenya, Senegal, South Africa, and Uganda*. Pollicy. August. http://ogbv.pollicy.org/legal_analysis.pdf.

Odeh, Shahrazad. 2018. *A Violent Network: Gender-Based Violence Against Palestinian: Women in Virtual Space*. 7amleh — The Arab Center for the Advancement of Social Media. November. https://7amleh.org/wp-content/uploads/2018/11/Report_GBV_-_KtK.pdf.

Office of the Council of Europe Commissioner for Human Rights. 2021. "Human Rights of LGBTI People in Europe: Current Threats to Equal Rights, Challenges Faced by Defenders, and the Way Forward." Online event, February 9. https://rm.coe.int/human-rights-of-lgbti-people-in-europe-current-threats-to-equal-rights/1680a4be0e.

Office of the United Nations High Commissioner for Human Rights. 2021. "The Gender Digital Divide Is a Reflection of the Overall Discrimination Faced by Women and Girls, High Commissioner for Human Rights Tells Human Rights Council." Press release, September 27. www.ohchr.org/en/press-releases/2021/09/gender-digital-divide-reflection-overall-discrimination-faced-women-and.

Oliver, Kelly. 2015. "Rape as Spectator Sport and Creepshot Entertainment: Social Media and the Valorization of Lack of Consent." *American Studies Journal* (10): 1–16. https://philpapers.org/rec/OLIRAS.

O'Malley, Roberta Liggett and Karen M. Holt. 2022. "Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime." *Journal of Interpersonal Violence* 37 (1–2): 258–83. https://doi.org/10.1177/0886260520909186.

Ontario Human Rights Commission. 2014. "Policy on preventing discrimination because of gender identity and gender expression." www.ohrc.on.ca/en/policy-preventing-discrimination-because-gender-identity-and-gender-expression.

Oswald, Flora, Alex Lopes, Kaylee Skoda, Cassandra L. Hesse and Cory L. Pedersen. 2020. "I'll Show You Mine so You'll Show Me Yours: Motivations and Personality Variables in Photographic Exhibitionism." *The Journal of Sex Research* 57 (5): 597–609. https://doi.org/10.1080/00224499.2019.1639036.

Padte, Richa Kaul and Anja Kovacs. 2013. "Keeping women safe? Gender, online harassment and Indian law." Internet Democracy Project, June 29. https://internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law.

Paola, Steffania, Constanta Figueroa, Juliana Guerra, Rocío Consales, Violeta Cereceda and Vladimir Garay. 2017. *Latin America in a Glimpse: Gender, Feminism and the Internet in Latin America*. Derecos Digitales. November. www.derechosdigitales.org/wp-content/uploads/GlImpse2017_eng.pdf.

Palumbo, Mariana and Delfina Schenone Sienra. 2017. "EROTICS Global Survey 2017: Sexuality, rights and internet regulations." APC. December 19. www.apc.org/en/pubs/erotics-global-survey-2017-sexuality-rights-and-internet-regulations.

Parsons, Christopher, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo and Ronald Deibert. 2019. *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. Research Report No. 119. June. The Citizen Lab. https://citizenlab.ca/docs/stalkerware-holistic.pdf.

Philip, Shannon. 2018. "Youth and ICTs in a 'new' India: exploring changing gendered online relationships among young urban men and women." *Gender & Development* 26 (2): 313–24. https://doi.org/10.1080/13552074.2018.1473231.

Posetti, Julie. 2017. "Fighting back against prolific online harassment: Maria Ressa." In *An Attack on One is an Attack on All*, edited by Larry Kilman, 37–40. Paris, France: UNESCO. https://en.unesco.org/an-attack-on-one.

Posetti, Julie and Nabeelah Shabbir. 2022. *The Chilling: What More Can News Organisations Do to Combat Gendered Online Violence?* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000383043.locale=en.

Posetti, Julie, Nermine Aboulez, Kalina Bontcheva, Jackie Harrison and Silvio Waisbord. 2020. "Online Violence against Women Journalists: A Global Snapshot of Incidence and Impacts." International Center for Journalists and UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000375136.

Posetti, Julie, Nabeelah Shabbir, Diana Maynard, Kaline Bontcheva and Nermine Aboulez. 2021. "The Chilling: Global Trends in Online Violence against Women Journalists." Research Discussion Paper. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000377223/PDF/377223eng.pdf.multi.

Powell, Anastasia and Nicola Henry. 2015. "Digital Harassment and Abuse of Adult Australians: A Summary Report." RMIT University. www.parliament.nsw.gov.au/lcdocs/other/7351/Tabled%20Document%20-Digital%20Harassment%20and%20Abuse%20of%20A.pdf.

———. 2016. "Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives." *Policing and Society* 28 (3): 291–307. https://doi.org/10.1080/10439463.2016.1154964.

———. 2017. *Sexual Violence in a Digital Age*. London, UK: Palgrave MacMillan. https://link.springer.com/book/10.1057/978-1-137-58047-4.

Powell, Anastasia, Adrian J. Scott, Asher Flynn and Nicola Henry. 2020. "Image-based sexual abuse: An international study of victims and perpetrators." Summary Report. RMIT University. https://research.monash.edu/en/publications/image-based-sexual-abuse-an-international-study-of-victims-and-pe.

Radhakrishnan, Radhika. 2020. "'I took Allah's name and stepped out': Bodies, Data and Embodied Experiences of Surveillance and Control During COVID-19 in India." Data Governance Network Working Paper 12. Internet Democracy Project, November 12. https://internetdemocracy.in/reports/i-took-allahs-name-and-stepped-out-bodies-data-and-embodied-experiences-of-surveillance-and-control-during-covid-19-in-india.

Ramaseshan, Geeta, Sudaroli Ramasamy, M. R. Sangeetha, S. Prabha, Nandita Krishna and, Shreeja Kumar. 2019. "Towards a safer cyberzone: A study on gender and online violence in Tamil Nadu." IT For Change. https://itforchange.net/sites/default/files/add/TamilNadu-Report_Righting-Gender-Wrongs.pdf.

Ramos, Raphaela . 2020. "Violência contra a mulher na internet cresce na quarentena. Saiba como identificar e se defender." *O Globo Celina*, May 22. https://oglobo.globo.com/celina/violencia-contra-mulher-na-internet-cresce-na-quarentena-saiba-como-identificar-se-defender-1-24438989.

Reporters Without Borders. 2018a. *Online Harassment of Journalists: Attack of the Trolls*. https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf.

———. 2018b. *Women's Rights: Forbidden Subject*. Paris, France: Reporters Without Borders. https://rsf.org/sites/default/files/womens_rights-forbidden_subject.pdf.

Ribeiro, Manoel Horta, Raphael Ottoni, Robert West, Virgílio A. F. Almeida and Wagner Meira Jr. 2020. "Auditing radicalization pathways on YouTube." *FAT '20: Proceedings of the 2020 Conference on Fairness, Accountability and Transparency*, 131–41.

Ruiz, Juliana Pacetta, Mariana Giorgetti Valente and Natália Neris. 2019. "Between the perpetrator and the victim: the role of Internet ontermediaries on violations against women." *Sociology & Technoscience* 9 (1): 9–27.

Ryakitimbo, Rebecca. 2018. "Meltdown of Protections for Data and Privacy in Tanzinia for LGBTQIA and Others." GenderIT, November 15. www.apc.org/en/blog/meltdown-protections-data-and-privacy-tanzania-lgbtqia-and-others.

Sallam, Yara. 2018. "Online Violence Faced by Outspoken Activists: The Case from Egypt." GenderIt, June 20. www.genderit.org/feminist-talk/online-violence-faced-outspoken-activists-case-egypt.

Sambasivan, Nithya, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytan-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill and Sunny Consolvo. 2019. "'They Don't Leave Us Alone Anywhere We Go': Gender and Digital Abuse in South Asia." CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–14. https://doi.org/10.1145/3290605.3300232.

Sambuli, Nanjira, Ana Brandusescu and Ingrid Brudvig. 2018. "Advancing Women's Rights Online: Gaps and Opportunities in Policy and Research." World Wide Web Foundation. August. http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf.

Sanya, Brenda Nyandiko. 2013. "Disrupting patriarchy: An examination of the role of e-technologies in rural Kenya." *Feminist Africa* 18: 12–24. https://feministafrica.net/wp-content/uploads/2019/10/features_disrupting_patriarchy.pdf.

Scheim, Ayden I. and Greta R. Bauer. 2019. "Sexual Inactivity Among Transfeminine Persons: A Canadian Respondent-Driven Sampling Survey." *The Journal of Sex Research* 56 (2): 264–71. https://doi.org/10.1080/00224499.2017.1399334.

Segal, Murray D. 2015. *Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case.* https://novascotia.ca/segalreport/Parsons-Independent-Review.pdf.

Sequera, Maricarmen. 2021. "Non-Consensual Image Dissemination in Paraguay: An Exploratory Research." TEDIC. June 7. www.tedic.org/wp-content/uploads/2021/06/Imagen-no-consentida-Tedic-web-EN.pdf.

Sey, Araba and Nancy Hafkin, eds. 2019. *Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership*. Report of EQUALS Research Group, led by the United Nations University. March. https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf.

Shanahan, Matthew. 2022. *The Mobile Gender Gap Report.* GSMA Intelligence. June. www.gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-Gap-Report-2022.pdf.

Shariff, Shaheen and Karen Eltis. 2017. "Addressing Online Sexual Violence: An Opportunity for Partnerships between Law and Education." *Education & Law Journal* 27 (1): 99–117.

Silva, Ilena. 2022. "Towards a feminist framework for AI development: from principles to practice." Derechos Digitales, August 16. www.derechosdigitales.org/publicaciones/towards-a-feminist-framework-for-ai-development-from-principles-to-practice/.

Silva, Jason and Emily Ann Greene-Colozzi. 2019. "Fame-seeking mass shooters in America: severity, characteristics, and media coverage." *Aggression and Violent Behavior* (48): 24–35. https://doi.org/10.1016/j.avb.2019.07.005.

Sívori, Horacio and Bruno Zilli. 2022. "Anti-rights Discourse in Brazilian Social Media: Digital Networks, Violence and Sex Polictics." Latin American Center on Sexuality and Human Rights, March 10. www.apc.org/en/pubs/anti-rights-discourse-brazilian-social-media-digital-networks-violence-and-sex-politics.

Slane, Andrea and Ganaele Langlois. 2016. "Regulating Business Models that Capitalize on User Posted Personal Information of Others: How Can Canada's Privacy Regime Protect Victims of Online Shaming Businesses?" August. www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_01/.

Sobieraj, Sarah. 2017. "Bitch, slut, skank, cunt: patterned resistance to women's visibility in digital publics." *Information, Communication & Society* 21 (11): 1700–14. https://doi.org/10.1080/1369118X.2017.1348535.

———. 2020. *Credible Threat: Attacks Against Women Online and the Future of Democracy*. New York, NY: Oxford University Press.

Strand, Cecilia and Jakob Svensson. 2021. "Disinformation campaigns about LGBTI+ people in the EU and foreign influence." European Parliament Briefing. July. www.europarl.europa.eu/RegData/etudes/BRIE/2021/653644/EXPO_BRI(2021)653644_EN.pdf.

Sugiura, Lisa. 2021. "Legitimising Misogyny." In *The Incel Rebellion: The Rise of the Manosphere and the Virtual War Against Women*, 95–115. Bingley, UK: Emerald.

Suzor, Nicolas, Molly Dragiewicz, Bridget Harris, Rosalie Gillett, Jean Burgess and Tess Van Geelen. 2019. "Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online." *Policy & Internet* 11 (1): 84–103. https://doi.org/10.1002/poi3.185.

Tabachnick, Barbara G. and Linda S. Fidell. 2019. *Using Multivariate Statistics*. 7th ed. New York, NY: Pearson Education.

TGEU. 2021. "TMM Update TDoR 2021." November 11. https://transrespect.org/en/tmm-update-tdor-2021/.

Thomasen, Kristen. 2018. "Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation." *Canadian Journal of Law and Technology* 16 (2): 307–28. https://digitalcommons.schulichlaw.dal.ca/cjlt/vol16/iss2/4/.

Thomasen, Kristen and Suzie Dunn. 2021. "Reasonable Expectations of Privacy in an Era of Drones and Deepfakes: Expanding the Supreme Court of Canada's Decision in *R v Jarvis*." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Asher Flynn, Nicola Henry and Jane Bailey, 555–76. Bingley, UK: Emerald. https://doi.org/10.1108/978-1-83982-848-520211040.

Thoreson, Ryan and Sam Cook, eds. 2011. *Nowhere to Turn: Blackmail and Extortion of LGBT People in Sub-Saharan Africa*. International Gay and Lesbian Human Rights Commission. www.world-psi.org/en/nowhere-turn-blackmail-and-extortion-lgbt-people-sub-saharan-africa.

Trans PULSE. 2011. "We've Got Work to Do: Workplace Discrimination and Employment Challenges for Trans People in Ontario." Trans PULSE E-Bulletin, May 30.

Treuthart, Mary Pat. 2019. "Connectivity: The Global Gender Digital Divide and Its Implications for Women's Human Rights and Equality." *Gender and International Law* 23 (1): 1–54. https://gjil.scholasticahq.com/article/12338-connectivity-the-global-gender-digital-divide-and-its-implications-for-women-s-human-rights-and-equality.

Trevisan, João Silvério. 2018. *Devassos no Paraíso: A homossexualidade no Brasil, da colônia à atualidade*. 4th ed. Rio de Janeiro, Brazil: Objetiva.

Tucker, Nia. 2020. "COVID-19 is Leaving Women and LGBTQIA+ People in the USA Vulnerable to Online Surveillance." GenderIT, August 5. https://genderit.org/feminist-talk/covid-19-leaving-women-and-lgbtqia-people-usa-vulnerable-online-surveillance.

Tyers-Chowdhury, Alexandra and Gerda Binder. 2021. "What we know about the gender digital divide for girls: A literature review." UNICEF Gender and Innovation Evidence Briefs. www.unicef.org/eap/reports/innovation-and-technology-gender-equality-0.

Udwadia, Zarah and Baldeep Grewal. 2019. "Free to Be Mobile: Ensuring That Women, Girls, Queer and Trans Persons Can Inhabit Digital Spaces Freely and Fearlessly." Point of View, March 11. www.apc.org/en/pubs/free-be-mobile-ensuring-women-girls-queer-and-trans-persons-can-inhabit-digital-spaces-freely.

Uhl, Carolyn A., Katlin J. Rhyner, Cheryl A. Terrance and Noel R. Lugo. 2018. "An examination of nonconsensual pornography websites." *Feminism & Psychology* 28 (1): 50–68. https://journals.sagepub.com/doi/10.1177/0959353517720225.

UN Committee on the Elimination of Discrimination against Women. 2017. "General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19." CEDAW/C/GC/35. July 14. https://digitallibrary.un.org/record/1305057?ln=en.

UN Women. 2022. "Toolkit: Youth Guide to End Online Gender-Based Violence." December 14. https://asiapacific.unwomen.org/sites/default/files/2022-12/Youth-Toolkit_14-Dec_compressed-final.pdf.

———. 2023a. *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls*. Expert guidance and substantive inputs to preparations for the 67th Session of the Commission on the Status of Women. March 18. www.unwomen.org/sites/default/files/2023-02/CSW67-Expert-Group-Meeting-report-en.pdf.

———. 2023b. *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls*. Agreed Conclusions. 67th Session of the Commission on the Status of Women. March 20. www.unwomen.org/en/csw/csw67-2023/session-outcomes.

United Nations. 2018. "UN experts call on India to protect journalist Rana Ayyub from online hate campaign." Press release, May 24. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23126&LangID=E.

———. 2022. "Defenders of the human rights of LGBT persons constantly at risk, warn UN experts." Statement, March 24. www.ohchr.org/en/statements/2022/03/defenders-human-rights-lgbt-persons-constantly-risk-warn-un-experts.

United Nations General Assembly. 2018. "Report of the Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity." A/73/152. https://digitallibrary.un.org/record/1639754?ln=en.

United Nations Human Rights Council. 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." A/HRC/38/47. June 18. https://digitallibrary.un.org/record/1641160.

United Nations Population Fund. 2021. *Technology-facilitated Gender-based Violence: Making all spaces safe*. December. www.unfpa.org/sites/default/files/pub-pdf/UNFPA-TFGBV-Making%20All%20Spaces%20Safe.pdf.

US Department of State. 2022. "2022 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse." March 16. www.state.gov/2022-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/.

Vaillancourt, Tracy, Heather Brittain, Amanda Krygsman, Ann H. Farrell, Sally Landon and Debra Pepler. 2021. "School bullying before and during COVID-19: Results from a population-based randomized design." *Aggressive Behavior* 47 (5): 557–69. https://doi.org/10.1002/ab.21986.

Valente, Mariana. 2018. "Do We Need New Laws to Address Non-Consensual Circulation of Intimate Images: The Case of Brazil." GenderIT, June 17. www.genderit.org/articles/do-we-need-new-laws-address-non-consensual-circulation-intimate-images-case-brazil.

Valente, Mariana Giorgetti, Natália Neris, Juliana Pacetta Ruiz and Lucas Bulgarelli. 2016. *The Body is the Code: Legal Strategies to Combat Revenge Porn in Brazil*. São Paulo, Brazil: Internet Lab.

Van Der Wilk, Adriane. 2018. *Cyber violence and hate speech online against women*. Policy Department for Citizen's Rights and Constitutional Affairs. PE 604.979. September. www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf.

Vashistha, Aditya, Abhinav Garg, Richard Anderson and Agha Ali Raza. 2019. "Threats, Abuses, Flirting, and Blackmail: Gender Inequity in Social Media Voices Forums." CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3290605.3300302.

Vasudevan, Amrita. 2018. *Report of the National Dialogue on Gender-Based Cyber Violence*. IT for Change. https://projects.itforchange.net/e-vaw/wp-content/uploads/2018/03/Event-Report-of-National-Dialogue-on-Gender-Based-Cyber-Violence.pdf.

Villamil, Daniela García. 2022. "Advancing gender equality and women's digital empowerment in the Global South." Policy Brief No. 14. Southern Voice, September 30. http://southernvoice.org/advancing-gender-equality-and-womens-digital-empowerment-in-the-global-south.

Virupaksha, H. G., Daliboyina Muralidhar and Jayashree Ramakrishna. 2016. "Suicide and Suicidal Behavior among Transgender Persons." *Indian Journal of Psychological Medicine* 38 (6): 505–09. https://doi.org/10.4103/0253-7176.194908.

Vogels, Emily A. 2021. *The State of Online Harassment*. Pew Research Center. January 31. www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf.

Waisbord, Silvio. 2020. "Mob Censorship: Online Harassment of US Journalists in Times of Digital Hate and Populism." *Digital Journalism* 8 (8): 1030–1046. https://doi.org/10.1080/21670811.2020.1818111.

Waldman, Ari Ezra. 2019. "Law, Privacy, and Online Dating: 'Revenge Porn' in Gay Online Communities." *Law & Social Inquiry* 44 (4): 987–1018. www.cambridge.org/core/journals/law-and-social-inquiry/article/law-privacy-and-online-dating-revenge-porn-in-gay-online-communities/BCCE05CF25AA4C2E05CCF8D64980E839.

Ward, Zara. 2021. "Intimate image abuse, an evolving landscape." Revenge Porn Helpline. https://revengepornhelpline.org.uk/assets/documents/intimate-image-abuse-an-evolving-landscape.pdf?_=1639471939.

Wells, Georgia, Jeff Horwitz and Deepa Seetharaman. 2021. "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show." *The Wall Street Journal*, September 14. www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

Wilton Park. 2022. *Building a shared agenda on the evidence base for Gender-Based Online Harassment and Abuse* WP3057.

Wittes, Benjamin, Cody Poplin, Quinta Jurecic and Clara Spera. 2016. "Sextortion: Cybersecurity, teenagers, and remote sexual assault." Center for Technology Innovation at Brookings, May 11. www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/.

Wolak, Janis and David Finkelhor. 2016. "Sextortion: Findings from a survey of 1,631 victims." Crimes Against Children Research Centre. https://calio.dspacedirect.org/handle/11212/3037.

Woodlock, Delanie. 2017. "The Abuse of Technology in Domestic Violence and Stalking." *Violence Against Women* 23 (5): 584–602. https://doi.org/10.1177/1077801216646277.

Woodlock, Delanie, Karen Bentley, Darcee Schulze, Natasha Mahoney, Donna Chung and Amy Pracilio. 2020. *Second National Survey on Technology Abuse and Domestic Violence in Australia*. WESNET. November. https://wesnet.org.au/about/research/2ndnatsurvey/.

World Health Organization. 2021. "Violence against women." Fact sheet. March 9. www.who.int/news-room/fact-sheets/detail/violence-against-women.

World Wide Web Foundation. 2022a. *Strengthening Accountability for Online Gender-Based Violence: One Year Later.* https://webfoundation.org/research/strengthening-accountability-for-online-gender-based-violence-one-year-later/.

———. 2022b. *Gender and ICT Policy Playbook.* September 12. https://webfoundation.org/research/gender-and-ict-policy-playbook/.

Yahaya, Mardiya Siba and Neema Iyer. 2022. *(In)Visible: The Digital Threats Muslim Women Human Rights Defenders Face in the Greater Horn of Africa.* Pollicy and Musawah. May. www.musawah.org/wp-content/uploads/2022/05/InVisible-The-Digital-Threats-Muslim-Women-Human-Rights-Defenders-Face-in-the-Greater-Horn-of-Africa.pdf.

Young, Hilary and Emily Laidlaw. 2020. "Creating a Revenge Porn Tort for Canada." *Supreme Court Law Review.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3586056.

Younes, Rasha. 2021. "'Clean the streets of faggots': governments in the Middle East & North Africa target LGBT people via social media." The Conversationalist, August 5. https://conversationalist.org/2021/08/05/clean-the-streets-of-faggots-governments-in-the-middle-east-north-africa-target-lgbt-people-via-social-media/.

YWCA Canada. 2015."Creating a safer digital world for young women: Project Shift Needs Assessment Report Summary." September. https://ywcacanada.ca/wp-content/uploads/2019/05/Project-Shift_Needs-Assessment-Report-Summary.pdf.

Zagloul, Nancy M., Rasha M. Farghaly, Hossam ELKhatib, Sahar Y. Issa and Safaa M. El-Zoghby. 2022. "Technology facilitated sexual violence: a comparative study between working and non-working females in Egypt before and during the COVID-19 pandemic." *Egyptian Journal of Forensic Sciences* 12 (1): 21. https://doi.org/10.1186/s41935-022-00278-2.

Zaman, Sarah. 2022. "Pakistan's Progressive Transgender Law Faces Opposition 4 Years Later." Voice of America News, September 28. www.voanews.com/a/pakistan-s-progressive-transgender-law-faces-opposition-4-years-later-/6768168.html.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York, NY: PublicAffairs.

Appendix

Notes for tables:

a Full sample of participants who responded to a given question

b Subsample of participants who reported gender and sexual orientation (multi-way frequency analysis) and responded to a given question

c Partial chi-square (multi-way frequency analysis)

d See text for statistically significant differences

e z-test examined in order to fully explore three-way interaction

H. = Heterosexual

NS = not statistically significant $p<.05$

Analyses based on weighted cases

Table A1: Experiences with Forms of Online Harm

Incidents	Full Sample (%)[a]	Form x Gender x Sexual Orientation[b]	Form x Gender[c]	Form x Sexual Orientation[c]	Gender[d]			Sexual Orientation		Interaction[d]		
					Women	Men	Transgender and Gender-Diverse People	Hetero-sexual	LGB+	Women	Men	Transgender and Gender-Diverse People
Any form of online harm	59.7	$\chi^2(2, 12001)=6.193$, $p=.045$	$\chi^2(2, 12001)=13.307$, p=.001	$\chi^2(1, 12001)=126.611$, p<.001	59.9	57.0	67.8	57.2	75.8	H. = 58.6 LGB+ = 76.7	H. = 55.7 LGB+ = 72.6	H. = 57.4 LGB+ = 87.7
Repeated unwanted contact	37.7	NS	$\chi^2(2, 11846)=84.873$, $p<.001$	$\chi^2(1, 11846)=49.535$, $p<.001$	39.4	31.3	40.3	34.6	46.3	Not examined		
Unsolicited sexual images	28.1	NS	$\chi^2(2, 11865)=57.055$, $p<.001$	$\chi^2(1, 11865)=95.585$, $p<.001$	28.9	22.8	31.1	24.8	40.1	Not examined		
Unauthorized access	24.5	NS	NS	$\chi^2(1, 11881)=30.530$, $p<.001$	Not examined			24.1	32.8	Not examined		
Discrimination	19.8	NS	$\chi^2(2, 11884)=8.361$, $p=.015$	$\chi^2(1, 11884)=173.587$, $p<.001$	17.8	18.8	30.6	17	36.6	Not examined		
Untrue information	17.8	$\chi^2(2, 11866)=11.728$, $p=.003$	$\chi^2(2, 11866)=30.784$, $p<.001$	$\chi^2(1, 11866)=64.723$, $p<.001$	16.5	19.8	30.1	17.4	29.3	H. = 15.3 LGB+ = 30.9	H. = 19.3 LGB+ = 25.5	H = 24.0 LGB+ = 41.8
Impersonation	16.5	NS	$\chi^2(2, 11881)=16.704$, $p<.001$	$\chi^2(1, 11881)=4.851$, $p=.028$	14.0	16.6	19.5	15.1	18.2	Not examined		
Identity-based harassment	16.3	NS	$\chi^2(2, 11867)=38.964$, $p<.001$	$\chi^2(1, 11867)=262.301$, $p<.001$	15.8	13.3	33.9	13.1	36.3	Not examined		
Monitored, tracked or spied on	14.7	$\chi^2(2, 11797)=7.466$, $p=.024$	$\chi^2(2, 11797)=24.297$, $p<.001$	$\chi^2(1, 11797)=13.860$, $p<.001$	12.5	14.6	24.0	13.3	18.6	H. = 11.9 LGB+ = 19.7	H. = 14.5 LGB+ = 15.5	H = 21.3 LGB+ = 29.1
Doxing	14.7	NS	$\chi^2(2, 11866)=50.582$, $p<.001$	NS	12.8	17.1	23.6	Not examined		Not examined		
Blackmail	12.1	NS	$\chi^2(2, 11885)=35.368$, $p<.001$	$\chi^2(1, 11885)=34.385$, $p<.001$	10.1	12.7	23.1	11.0	18.6	Not examined		
Networked harassment	11.8	$\chi^2(2, 11888)=7.396$, $p=.025$	$\chi^2(2, 11888)=50.859$, $p<.001$	$\chi^2(1, 11888)=56.919$, $p<.001$	9.3	11.5	27.8	9.9	19.6	H. = 8.5 LGB+ = 19.4	H. = 11.0 LGB+ = 18.1	H. = 26.7 LGB+ = 29.9
Physical threats	11.7	$\chi^2(2, 11878)=12.323$, $p=.002$	$\chi^2(2, 11878)=40.023$, $p<.001$	$\chi^2(1, 11878)=105.502$, $p<.001$	11.1	13.8	28.1	11.6	25.5	H. = 10.0 LGB+ = 25.4	H. = 13.1 LGB+ = 21.6	H. = 18.3 LGB+ = 47.4
Non-consensual distribution of intimate images	7.6	NS	$\chi^2(2, 11863)=28.780$, $p<.001$	$\chi^2(1, 11863)=73.145$, $p<.001$	6.7	8.4	19.2	7.0	16.6	Not examined		

Table A2: Reported Impacts of Online Harm

Impacts	Full Sample (% Very Negative)[a]	Impact x Gender x Sexual Orientation[b]	Impact x Gender[c]	Impact x Sexual Orientation[c]	Gender[d]			Sexual Orientation		Interaction[d]		
					Women	Men	Transgender and Gender-Diverse People	Hetero-sexual	LGB+	Women	Men	Transgender and Gender-Diverse People
Mental health	27.7	NS	χ^2 (2, 6870)=51.738, p<.001	χ^2(1, 6870)=37.711, p<.001	29.4	21.8	29.8	24.7	35.8	Not examined		
Personal reputation	24.7	NS	NS	NS	Not examined			Not examined		Not examined		
Ability to engage freely online	22.5	NS	χ^2 (2, 6809)=18.989, p<.001	NS	22.9	18.6	20.1	Not examined		Not examined		
Freedom to express political or personal views	21.7	NS	NS	χ^2(1, 6790)=10.680, p<.001	Not examined			19.5	25.5	Not examined		
Ability to focus	20.4	NS	χ^2(2, 6839)=18.524, p<.001	χ^2(1, 6839)=7.920, p<.005	19.8	16.3	26.4	17.8	22.9	Not examined		
Close relationships	20.3	NS	NS	χ^2(1, 6819)=5.897, p=.015	Not examined			17.9	24.2	Not examined		
Physical safety	19.3	χ^2(2, 6824)=7.166, p=.028	χ^2(2, 6824)=22.910, p<.001	χ^2(1, 6824)=13.931, p<.001	20.7	16.3	24.4	13.1	36.3	H. = 19.8 LGB+ = 27.8	H. = 15.5 LGB+ = 22.0	H. = 28.9 LGB+ = 18.2
Employment or business	18.0	NS	χ^2(2, 6767)=13.242, p=.001	NS	15.9	17.5	28.8	Not examined		Not examined		
Desire to live	16.8	NS	χ^2(2, 6792)=19.339, p<.001	χ^2(1, 6792)=26.866, p<.001	15.8	13.6	29.6	14.1	22.9	Not examined		
Sexual autonomy/ freedom	16.2	χ^2(2, 6728)=7.717 p=.021	χ^2(2, 6728)=16.159, p<.001	χ^2(2, 6728)=36.241, p<.001	16.8	14.6	28.4	14.9	25.1	H. = 16.4 LGB+ = 21.5	H. = 13.0 LGB+ = 26.9	H. = 23.8 LGB+ = 35.4

Table A3: Perceptions of Who OGBV Is a Big Problem For

Who OGBV is a big problem for	Full Sample (% Yes, "Very Big Problem")[a]	Problem for x Gender[b]	Gender (%)[c, d]		
			Women	Men	Transgender and Gender-Diverse People
Yourself	28.4	$\chi^2(2, 11490)=28.774$, $p<.001$	25.9	21.7	26.0
Men	22.7	$\chi^2(2, 10727)=27.665$, $p<.001$	22.3	18.2	19.0
Women	44.3	$\chi2(2, 11298)=105.811$, $p<.001$	47.7	38.1	38.1
LGBTQ+ people	46.5	$\chi2(2, 10753)=86.859$, $p<.001$	51.4	42.4	41.6

.

Table A4: Perceptions of the Harmfulness of Online Harms

Harmfulness	% of Full Sample "Extremely Harmful"[a]	Harmfulness x Gender x Sexual Orientation[b]	Harmfulness x Gender[c]	Harmfulness x Sexual Orientation[c]	Gender[d]			Sexual Orientation		Interaction [d]		
					Women	Men	Transgender and Gender-Diverse People	Hetero-sexual	LGB+	Women	Men	Transgender and Gender-Diverse People
Non-consensual distribution of intimate images	76.6	NS	$\chi^2(2, 11637)=235.435$, $p<.001$	NS	82.8	71.2	60.0	Not examined		Not examined		
Physical threats	74.4	$\chi^2(2, 11639)=13.498$, $p=.001$	$\chi^2(2, 11639)=265.219$, $p<.001$	$\chi^2(1, 11639)=4.461$, $p=.035$	80.5	68.0	56.1	74.7	70.2	H. = 81.4 LGB+ = 73.0	H. = 68.1 LGB+ = 70.4	H. = 59.2 LGB+ = 52.5
Blackmail	73.5	$\chi^2(2, 11653)=10.785$, $p=.005$	$\chi^2(2, 11653)=173.592$, $p<.001$	NS	77.8	67.4	58.3	72.9[e]	69.8[e]	H. = 78.5 LGB+ = 71.4	H. = 67.4 LGB+ = 70.0	H. = 58.2 LGB+ = 61.0
Impersonation	69.5	$\chi^2(2, 11670)=15.129$, $p=.001$	$\chi^2(2, 11670)=70.974$, $p<.001$	$\chi^2(1, 11670)=14.029$, $p<.001$	72.5	65.8	55.6	69.7	62.8	H. = 73.6 LGB+ = 61.2	H. = 66.1 LGB+ = 65.6	H. = 55.8 LGB+ = 57.0
Networked harassment	68.1	NS	$\chi^2(2, 11597)=195.089$, $p<.001$	NS	74.0	62.0	58.3	Not examined		Not examined		
Unauthorized access	68.0	$\chi^2(2, 11679)=24.438$, $p<.001$	$\chi^2(2, 11679)=91.422$, $p<.001$	NS	70.5	62.5	52.3	66.8[e]	63.1[e]	H. = 71.3 LGB+ = 60.0	H. = 62.4 LGB+ = 66.5	H. = 50.7 LGB+ = 59.5
Monitored, tracked or spied on	66.9	$\chi^2(2, 11600)=9.990$, $p=.007$	$\chi^2(2, 11600)=169.870$, $p<.001$	NS	71.5	60.6	53.6	66.5[e]	63.9[e]	H. = 72.4 LGB+ = 65.6	H. = 60.6 LGB+ = 63.2	H. = 52.1 LGB+ = 58.5
Doxing	65.4	$\chi^2(2, 11651)=7.060$, $p=.029$	$\chi^2(2, 11651)=134.585$, $p<.001$	NS	70.2	59.9	53.6	65.1[e]	66.1[e]	H. = 70.4 LGB+ = 67.6	H. = 59.8 LGB+ = 65.3	H. = 51.7 LGB+ = 61.3
Untrue information	65.0	$\chi^2(2, 11646)=10.796$, $p=.005$	$\chi^2(2, 11646)=88.154$, $p<.001$	$\chi^2(1, 11646)=9.121$, p=.003	67.9	59.3	53.0	64	58.3	H. = 68.5 LGB+ = 58.3	H. = 59.2 LGB+ = 60.2	H. = 57.2 LGB+ = 48.7
Unsolicitated sexual images	65.0	NS	$\chi^2(2, 11540)=297.277$, $p<.001$	$\chi^2(1, 11540)=25.004$, $p<.001$	70.4	54.9	53.2	63.5	54.6	Not examined		
Identity-based harassment	64.6	NS	$\chi^2(2, 11416)=206.839$, $p<.001$	NS	68.4	55.4	48.9	Not examined		Not examined		
Discrimination	60.5	NS	$\chi^2(2, 11609)=223.605$, $p<.001$	NS	64.9	51.2	48.1	Not examined		Not examined		
Repeated unwanted contact	49.9	$\chi^2(2, 11550)=6.386$, $p=.041$	$\chi^2(2, 11550)=171.896$, $p<.001$	$\chi^2(1, 11550)=12.535$, $p=.035$	55.6	43.4	43.8	50.2	43.8	H. = 56.5 LGB+ = 46.2	H. = 43.6 LGB+ = 42.2	H. = 49.0 LGB+ = 39.7

Table A5: Young People — Perceptions of the Harmfulness of Online Harms

Harmfulness	% of Full Sample "Extremely Harmful"[a]	Harmfulness x Age	Aged 16–25 Years	Aged 26–74 Years
Non-consensual distribution of intimate images	76.6	NS	Not examined	
Physical threats	74.4	$\chi^2(1, 17131)=14.486$, $p<.001$	72.2	75.1
Blackmail	73.5	$\chi^2(1, 17174)=33.510$, $p<.001$	70.0	74.6
Impersonation	69.5	$\chi^2(1, 17196)=169.632$, $p<.001$	61.2	72.0
Networked harassment	68.1	$\chi^2(1, 17055)=25.492$, $p<.001$	64.9	69.1
Unauthorized access	68.0	$\chi^2(1, 17187)=43.469$, $p<.001$	63.8	69.3
Monitored, tracked or spied on	66.9	$\chi^2(1, 17079)=3.917$, $p=.048$	65.6	67.3
Doxing	65.4	$\chi^2(1, 17121)=16.075$, $p<.001$	62.8	66.2
False information	65.0	$\chi^2(1, 17135)=102.449$, $p<.001$	58.4	67.1
Unsolicited sexual images	65.0	NS	Not examined	
Identity-based harassment	64.6	NS	Not examined	
Discrimination	60.5	$\chi^2(1, 17123)=15.408$, $p<.001$	57.9	61.3
Repeated unwanted contact	49.9	$\chi^2(1, 17063)=52.170$, $p<.001$	44.9	51.4

Table A6: High-Profile People — Experiences with Forms of Online Harm

Incident Type	Full Sample (%) [a]	High Profile x Incident	Not High Profile	High Profile
Any form of online harm	59.7	$\chi^2(1, 17817)=325.054$, $p<.001$	57.2	77.2
Reputation and identity-based harms	37.6	$\chi^2(1, 17785)=560.933$, $p<.001$	34.3	60.3
Any coercion and harassment	45.0	$\chi^2(1, 17789)=388.193$, $p<.001$	42.2	64.4
Any privacy and security-based harms	34.4	$\chi^2(1, 17767)=462.260$, $p<.001$	31.5	54.6
Any sexual harms	29.3	$\chi^2(1, 17650)=310.012$, $p<.001$	27.1	45.3

Table A7: Most Serious Incident — Frequency

Frequency of Incident(s)	Full Sample (% Chronic)[a]	Frequency x Gender x Sexual Orientation[b]	Frequency x Gender[c]	Frequency x Sexual Orientation[c]	Gender[d]			Sexual Orientation		Interaction		
					Women	Men	Transgender and Gender-Diverse People	Hetero-sexual	LGB+	Women	Men	Transgender and Gender-Diverse People
Chronic (monthly, weekly and daily) exposure	12.6	NS	$\chi^2(2, 6501)=8.078$, $p<.018$	$\chi^2(1, 6501)=11.552$, $p<.001$	13.7	14.3	25.5	13.5	19.3	Not examined		

Table A8: Most Serious Incident — Reason for Being Targeted

Reason	Full Sample (% Yes)[a]	Reason x Gender x Sexual Orientation[b]	Reason x Gender[c]	Reason x Sexual Orientation[c]	Gender[d]			Sexual Orientation		Interaction[d]		
					Women	Men	Transgender and Gender-Diverse People	Hetero-sexual	LGB+	Women	Men	Transgender and Gender-Diverse People
Your gender identity	24.5	NS	$\chi^2(2, 7039)=199.627$, $p<.001$	$\chi^2(1, 7039)=9.351$, $p<.002$	29.8	16.0	25.5	23.0	28.7	Not examined		
Your gender expression	8.3	NS	$\chi^2(2, 7039)=23.069$, $p<.001$	$\chi^2(1, 7039)=50.622$, $p<.002$	8.2	8.6	24.0	7.8	17.8	Not examined		
Your race/ethnicity	14.5	NS	$\chi^2(2, 7039)=89.876$, $p<.001$	NS	9.7	17.6	17.0	Not examined		Not examined		
Your age	13.5	NS	NS	NS	Not examined			Not examined		Not examined		
Your sexual orientation	7.0	$\chi^2(2, 7039)=7.723$, $p=.021$	$\chi^2(2, 7039)=38.886$, $p<.001$	$\chi^2(1, 7039)=585.192$, $p<.001$	7.9	12.2	25.7	6.6	42.7	H. = 5.4 LGB+ = 32.6	H. = 7.8 LGB+ = 53.3	H. = 11.2 LGB+ = 42.3
Your religion	12.1	NS	$\chi^2(2, 7039)=70.390$, $p<.001$	NS	7.7	13.9	14.1	Not examined		Not examined		
Your disability	3.5	NS	$\chi^2(2, 7039)=36.480$, $p<.001$	NS	2.7	5.4	7.0	Not examined		Not examined		

About the Authors

Suzie Dunn is a senior fellow at CIGI. She is an assistant professor at Dalhousie University's Schulich School of Law in Halifax, Nova Scotia. Her research centres on the intersections of gender, equality, technology and the law, with a specific focus on technology-facilitated gender-based violence (TFGBV), the non-consensual distribution of intimate images and impersonation in digital spaces. As a subject matter expert on TFGBV, Suzie has been a key contributor to CIGI's Supporting a Safer Internet project.

Tracy Vaillancourt is a senior fellow at CIGI. She is a Tier 1 Canada Research Chair in School-Based Mental Health and Violence Prevention at the University of Ottawa (uOttawa). She is cross-appointed as a full professor in counselling psychology, the Faculty of Education and the School of Psychology, Faculty of Social Sciences. At uOttawa, Tracy is a member of the Brain and Mind Institute, Faculty of Medicine, and the Centre for Health Law, Policy and Ethics with the Faculty of Law. She is the president of the International Society for Research on Aggression, a fellow and chair of the Royal Society of Canada Task Force on COVID-19, and the chief editor of the Child Mental Health and Interventions sections of *Frontiers in Child and Adolescent Psychiatry*.

Heather Brittain is a Vanier Scholar who is completing her doctoral degree in the Faculty of Education at the University of Ottawa in Tracy Vaillancourt's Brain and Behaviour Laboratory. She obtained master's degrees in education and statistics. Heather's research is focused on how the experience of childhood adversity, such as being the victim of peer abuse, impacts academic functioning and how these experiences relate to functional outcomes during adulthood, such as post-secondary educational success and job stability for women and men.

Acronyms and Abbreviations

AI	artificial intelligence
APC	Association for Progressive Communications
CIGI	Centre for International Governance Innovation
G20	Group of Twenty
IPV	intimate partner violence
ITU	International Telecommunication Union
LEAF	Women's Legal Education and Action Fund
LGB+	lesbian, gay, bisexual or other non-heterosexual sexual orientations
LGBTQ+	lesbian, gay, bisexual, transgender, queer or questioning and other non-heterosexual sexual orientations, and gender-diverse identities
MFA	multi-way frequency analysis
MP	member of Parliament
NCDII	non-consensual distribution of intimate images
OGBV	online gender-based violence
STEM	science, technology, engineering and math
TFGBV	technology-facilitated gender-based violence
TFV	technology-facilitated violence
UAE	United Arab Emirates
UNESCO	United Nations Educational, Scientific and Cultural Organization

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline