



Photo credit: CR Shelare, Shutterstock, April 2016

Navigating Uncharted Waters: Curbing the Global Threat of Cyberviolence

Nicholas Metheny, Renu Sara Nargund, Flavia Bustreo and Felicia Knaul

It is undeniable that the proliferation of internet access and internet-connected mobile devices has improved health-care access and health outcomes for marginalized populations worldwide. Internet use has been associated with improved access to health care,¹ better health literacy,² and access to social norms that promote health equity.³ While the fastest uptake of the internet is currently in Africa and Asia, its use in low- and middle-income countries is far from universal and is often stratified along longstanding class, ethnic, racial, and gender lines. It is therefore in these countries where the digital divide

between those with internet access and those without it is most stark, especially among adolescent girls and women.⁴

In addition to the digital divide, other disadvantages of increased connectivity are emerging. Among them, cyberviolence—antisocial, aggressive, and violent content and behaviors that include but are not limited to physical threats, sexual harassment, sex trolling,⁵ doxing,⁶ and nonconsensual pornography⁷—is an all-too-common and an increasingly dark side to the proliferation of internet use globally.

About the Series

Gender-based violence (GBV) affects one in three women worldwide, making it an urgent and important policy challenge. Many countries around the world have passed laws intended to protect women from violence, yet violence persists. Over the past year, the COVID-19 pandemic has raised awareness of the perils women face from gender-based violence—what has come to be known as the “shadow pandemic”—but it has also aggravated risk factors while increasing barriers to protection, support, and justice.

This publication aims to focus on the intersection of gender-based violence and the rule of law by examining how legal frameworks, judicial system responses, and public policy contribute to the ways in which gender-based violence is—and is not—addressed around the world. Each piece addresses the complicated challenge of gender-based violence and the successes and failures of various public policy responses globally, and offers recommendations for a path forward.

Cyberviolence affects all countries: It follows the spread of the internet in high-income countries and throughout the Global South. More than half of girls and young women ages 15 to 25 reported being the victims of cyberviolence, according to a Plan International report based on research involving more than 14,000 women from 22 countries.⁸ Further, the risk is increasing with COVID-19. The pandemic has shifted numerous social, educational, and work-related activities online, further increasing internet use. Children’s increased online exposure is of particular concern, as cyber abuse typically begins early in life: It is estimated that 1 in 10 girls with access to the internet experience at least one form of cyberviolence before the age of 15.⁹

“Marginalized groups are often singled out for cyberviolence on the basis of their identities.”

Like other forms of violence, cyberviolence intersects with the social determinants of health—poverty, education, gender inequality, and other forms of interpersonal violence.¹⁰ Those at the highest risk of cyberviolence are those who are already at an increased risk of physical and sexual violence that stems from an imbalance of power between the victim and perpetrator: women, girls, LGBTIQ¹¹ people, those with disabilities, and racial and ethnic minorities. Further, marginalized groups are often singled out for cyberviolence on the basis of their identities. More than 40 percent of respondents in the 22-country study who identified as LGBTIQ said they were harassed online for their sexual or gender identity; 37 percent of girls who belonged to racial or ethnic minorities were harassed due to their racial or ethnic identity; and 14 percent of those indicating they had a disability had been bullied or harassed online specifically because of their disability.¹²

Cyberviolence can lead to serious health consequences. Victims report trouble sleeping, fear for personal safety, reduced self-esteem, and feelings of powerlessness.¹³ The suffering of survivors can lead to serious mental and physical health outcomes, including depression, anxiety, social isolation, suicidal ideation, and self-harm behaviors.^{14, 15, 16}

“Governments have been slow to adopt and enforce regulations that curb online abuse and hold perpetrators accountable.”

Cyberviolence also blunts economic development both at an individual and country level—so much so that the United Nations has named it a significant reason for the growing gender digital divide.¹⁷ According to one study, nearly half¹⁸ of those experiencing cyberviolence reduced their online presence or left platforms altogether. This suggests that cyberviolence is exacerbating the already significant gap in online access and participation between men and women.

Though many have recognized that cyberviolence is widespread and harmful,¹⁹ governments have been slow to adopt and enforce regulations that curb online abuse and hold perpetrators accountable. To do so requires a multipronged approach that includes elements of primary and secondary prevention. First, governments and the technology platforms on which the majority of cyberviolence takes place should work together to keep violent content aimed at individuals off of the internet. In the United States (where many major platforms’ headquarters are located) President Biden’s forthcoming Task Force on Online Abuse and Harassment is part of a wider effort to regulate the production and sharing of violent social media and other online content, as well as to streamline reporting processes for those who en-

counter this type of content.²⁰ The European Union is pushing for an independent safeguarding entity to monitor and coordinate the response to cyberviolence.²¹ The entity would also serve as a regulatory body to which tech platforms would be obligated to report, and it would be given the authority to conduct external investigations of the causes of specific instances of cyberviolence and mandate companies to update mitigation techniques and strengthen content policies to help prevent these abuses from occurring.

In addition to fundamentally strengthening the frameworks and agencies that regulate the production of potentially harmful content, governments at all levels should consider passing legislation that holds perpetrators of cyberviolence accountable. Laws outlawing revenge porn have already been adopted across Europe and in 48 states in the United States.²² Unfortunately, due to opposition by powerful lobbies and a misunderstanding²³ of the nature of online abuse, many of these laws are written so narrowly as to be nearly useless.²⁴ The majority of them are limited to situations in which the perpetrator acted with the intent to personally harm the victim. But as with sexual assault, the important question is not intent, but consent. According to a study by the Cyber Civil Rights Initiative, nearly 80 percent of perpetrators of nonconsensual pornography indicate they did not act with the intent to harm the victim.²⁵ However, this in no way lessens the harmful impact of their actions. While children may be somewhat better protected legally, due to the widespread adoption of child exploitation statutes,²⁶ gaps in coverage, especially for teenage victims, remain. The legal landscape is similar in low- and middle-income countries (LMICs), most of which do not have laws against cyberviolence. Some LMIC countries (e.g., the Philippines,²⁷ India,²⁸ and South Africa²⁹) have made progress on legislating against specific acts of cyberviolence, but most LMICs lack the resources needed to enforce these laws. Globally, the functional limitations of existing laws in two areas—(1) the forms of cyberviolence that

are outlawed and (2) the restriction to perpetrators who are motivated by a personal desire to harm the victim—render the internet a breeding ground for cyberviolence.

“Countries must also consider whether marginalized groups may be disinclined to report cyberviolence due to other laws that may be hostile to their identities.”

Beyond resource availability, the effectiveness of cyberviolence laws greatly depends on the will and the ability to enforce them. According to one study of cyberviolence in India and the United States, police officers in both countries who were supposedly specially trained in cyberviolence enforcement were still unprepared to serve cyberviolence survivors or adequately pursue their perpetrators.³⁰ This speaks to a broader need to both better train those responsible for enforcing cyberviolence laws and ensure that survivors have access to strong support networks, including health-care providers, when they bring these crimes forward. Countries must also consider whether marginalized groups may be disinclined to report cyberviolence due to other laws that may be hostile to their identities. For instance, living in a country with regressive laws regarding homosexual behavior likely deters LGBTIQ victims of cyberviolence from reporting crimes committed against them. Existing at the intersection of other marginalized identities (e.g., racial, ethnic, ability, immigration status, religion) may similarly deter reporting.

Law enforcement must also confront the misconduct that occurs within its own ranks. Specific accountability measures for officer-perpetrated violence are imperative to the appropriate enforcement of cyberviolence laws. For example, the Interna-

tional Association of Chiefs of Police, a nonprofit association based in the United States, advocates for a zero-tolerance policy for police offenders.³¹

Despite the limitations and obstacles of legal reform, more laws against cyberviolence are needed. Just as pressure from international organizations, nongovernmental organizations, advocacy groups, and the media exists to outlaw marital rape in jurisdictions where it is not yet illegal,³² similar pressure should be mounted to outlaw cyberviolence. These efforts must come with an understanding of, and safeguards against, the disproportionate and often unjust ways in which the criminal legal system has affected historically excluded communities, which in many cases has driven those communities to mistrust the police and criminal legal apparatus. As the threat to women, girls, and other historically excluded communities continues to grow, it will be ever more important to prevent cyberviolence through comprehensive laws and policy reforms centered on the experiences of survivors. Until that happens, the true potential of widespread internet connectivity will remain unrealized.

NOTES

1. Lydia Ramsey, "How the Internet Is Improving Healthcare," World Economic Forum, January 3, 2017, <https://www.weforum.org/agenda/2017/01/technology-is-changing-the-way-we-view-our-health-this-is-how/>.
2. David Raths, "Expanding Internet Access Improves Health Outcomes," Government Technology, June 2020, <https://www.govtech.com/network/Expanding-Internet-Access-Improves-Health-Outcomes.html>.
3. Kathleen Stansberry, Janna Anderson, and Lee Raine, "4. The Internet Will Continue to Make Life Better," Pew Research Center, October 28, 2019, <https://www.pewresearch.org/internet/2019/10/28/4-the-internet-will-continue-to-make-life-better/>.
4. International Telecommunications Union, "Measuring Digital Development: Facts and Figures 2020," ITU Publications, 2020, <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf>.
5. "Sex trolling" definition: Intentionally instigating conflict, hostility, or arguments using intimate information about a person or their photos, videos, or other media without consent.
6. "Doxing" definition: The researching and broadcasting of personal (and often intimate) data.
7. "Nonconsensual pornography" definition: The distribution of sexually explicit imagery of individuals without their consent, also sometimes referred to as "revenge porn."
8. Plan International, "Free to Be Online? Girls' and Young Women's Experiences of Online Harassment," 2020 report, https://www.plan.de/fileadmin/website/05._Ueber_uns/Maedchenberichte/Maedchenbericht_2020/Free_to_be_online_report_englisch_FINAL.pdf.
9. European Institute for Gender Equality, "Cyber Violence against Women and Girls," June 23, 2017, <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>.
10. Cybercrime Convention Committee, "Mapping Study on Cyberviolence," Council of Europe, July 9, 2018, <https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c>.
11. "LGBTIQ" is an acronym for lesbian, gay, bisexual, transgender, intersex, and queer or questioning.
12. European Institute for Gender Equality, "Cyber Violence against Women and Girls," June 23, 2017, <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>.
13. Cybercrime Convention Committee, "Mapping Study on Cyberviolence," Council of Europe, July 9, 2018, <https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c>.
14. Michelle F. Wright, "Cyber Victimization on College Campuses: Longitudinal Associations with Suicidal Ideation, Depression, and Anxiety," *Criminal Justice Review* 41, no. 2 (June 2016), 190–203, <https://doi.org/10.1177/0734016816634785>.
15. *Institute of Medicine, Delivering High-Quality Cancer Care: Charting a New Course for a System in Crisis* (Washington, DC; The National Academies Press, 2013).

16. Randolph C. H. Chan, "Effects of Online Heterosexual Experiences on Physical and Mental Health in Sexual Minorities: An Examination of the Cognitive and Affective Mechanisms," *Journal of Interpersonal Violence*, June 9, 2021, <https://doi.org/10.1177/08862605211021962>.
17. United Nations General Assembly, "Promotion, Protection and Enjoyment of Human Rights on the Internet: Ways to Bridge the Gender Digital Divide from a Human Rights Perspective," United Nations High Commissioner for Human Rights, annual report, May 17, 2017, <https://undocs.org/A/HRC/35/9>.
18. Ibid.
19. Adriane Van Der Wilk, "Cyber Violence and Hate Speech Online against Women," European Parliament, August 2018, [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU\(2018\)604979_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf).
20. "The Biden Plan to End Violence against Women," Joe Biden for President: Official Campaign Website, <https://joebiden.com/vawa/>.
21. Cybercrime Convention Committee, "Mapping Study on Cyberviolence," Council of Europe, July 9, 2018, <https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c>.
22. "48 States + DC + One Territory Now Have Revenge Porn Laws," Cyber Civil Rights Initiative, <https://www.cybercivilrights.org/revenge-porn-laws/>.
23. Mary Anne Franks, "How to Defeat 'Revenge Porn': First, Recognize It's About Privacy, Not Revenge," HuffPost, June 22, 2016, https://www.huffpost.com/entry/how-to-defeat-revenge-porn_b_7624900.
24. Danielle Citron and Mary Anne Franks, "Evaluating New York's 'Revenge Porn' Law: A Missed Opportunity to Protect Sexual Privacy," Harvard Law Review Blog, March 19, 2019, <https://blog.harvardlawreview.org/evaluating-new-yorks-revenge-porn-law-a-missed-opportunity-to-protect-sexual-privacy/>.
25. Asia Eaton, Holly Jacobs, and Yanet Ruvalcaba, "2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration," Cyber Civil Rights Initiative, June 2017, <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>.
26. European Institute for Gender Equality "Cyber Violence against Women and Girls," June 23, 2017, <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>.
27. "An Act Defining and Penalizing the Crime of Photo and Video Voyeurism, Prescribing Penalties Therefore and for Other Purposes," Congress of the Philippines, Republic Act No. 9995, July 27, 2009, https://www.lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html.
28. Aditya Krishna, "Revenge Porn: Prosecution under the Current Indian Legal System," The Criminal Law Blog, National Law University, Jodhpur, April 13, 2020, <https://criminallawstudiesnluj.wordpress.com/2020/04/13/revenge-porn-prosecution-under-the-current-indian-legal-system/>.

29. Tom Head, "South Africa's New 'Revenge Porn' Laws: Here's What Will Land You in Jail," *The South African*, October 3, 2019, <https://www.thesouthafrican.com/news/what-is-revenge-porn-south-africa-laws-fines-jail-why/>.
30. Prit Kaur and Ranjay Vardhan, "Cyber Violence against Women and Girls (CVAWG): Preparedness of Cyber Units in Police Stations in United States of America and Women Police Stations in India," *Intellectual Quest*, Vol. 14 (December 2020), https://www.researchgate.net/publication/350671066_CYBER_VIOLENCE_AGAINST_WOMEN_AND_GIRLS_CVAWG_PREPAREDNESS_OF_CYBER_UNITS_IN_POLICE_STATIONS_IN_UNITED_STATES_OF_AMERICA_AND_WOMEN_POLICE_STATIONS_IN_INDIA.
31. "Domestic Violence by Police Officers: Model Policy," International Association of Chiefs of Police, July 2003, <https://www.theiacp.org/sites/default/files/all/d-e/DomesticViolencebyPolicePolicy.pdf>.
32. Ellen Wulffhorst, "UN Urges Countries to End Marital Rape and Close Legal Loophole," Thompson Reuters Foundation, June 26, 2019, <https://www.globalcitizen.org/en/content/un-women-marital-rape-laws/>.



Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

 www.wilsoncenter.org / gbv.wilsoncenter.org

 wwics@wilsoncenter.org

 facebook.com/woodrowwilsoncenter

 [@thewilsoncenter](https://twitter.com/thewilsoncenter)

 202.691.4000