2019

White paper series
issue 7

— COMBATING ONLINE —
VIOLENCE AGAINST WOMEN
A CALL FOR PROTECTION

OAS More rights for more people

Canada

— COMBATING ONLINE —

VIOLENCE AGAINST WOMEN

A CALL FOR PROTECTION

CREDITS

Luis Almagro
Secretary General
Organization of American States (OAS)

Farah Diva Urrutia
Secretary for Multidimensional Security

Alejandra Mora Mora
Executive Secretary
Inter-American Commission of Women (CIM)

Alison August Treppel
Executive Secretary
Inter-American Committee against Terrorism (CICTE)

Betilde Muñoz-Pogossian
Director of the Department of Social Inclusion

Technical Team

Belisario Contreras
Nathalia Foditsch
Kerry-Ann Barrett
Hilary Anderson
Pamela Molina
Claudia Gonzalez
Mariana Cardona
Miguel Angel Cañada
Rolando Ramirez
David Moreno

CONTENT

— COMBATING ONLINE —

VIOLENCE AGAINST WOMEN

A CALL FOR PROTECTION

Introduction

1

While about half of the world population is comprised of women **(World Bank, 2019)**, only 48% of them have access to the Internet (compared to 58% of men) **(ITU, 2019)**,[1] and this digital divide is worsened when a cross-cutting perspective is adopted, e.g. gender and race, ethnicity, disability, and age. This divide has important implications in terms of women's empowerment and development, as well as for societies, businesses, and economies. In addition to gaps in access, the lack of digital literacy skills is also a reality for many women.

The concept of digital literacy refers both to what technical skills are needed and to the ability to engage with online contents in a critical manner **(UNICEF, 2017)**. Further, **GSMA (2015)** has found, for example, that many women in developing countries do not grasp the depth and breadth of what the Internet could offer them in terms of content, as they are stuck in "application islands", meaning that what they understand to be "the Internet" is what they see through a limited number of mobile applications. Having proper digital literacy skills is key, especially considering that access to and use of the Internet has created many possibilities we would have never imagined. Undoubtedly, it has profoundly affected how we communicate, how we access information, how we understand our own identities.

By not having proper literacy, women are not fully aware of the risks involved in using the Internet. Indeed, despite the wide range of opportunities it brings, the adoption and use of the Internet has also been accompanied by challenges such as the need for strengthened privacy and security as our lives are increasingly lives through our online identities. One example of how women can be unwittingly exposed online is data leaks. In 2019, over 12 million medical records hosted by a governmental agency and related to women's reproductive health were exposed online in India. The issue was addressed by the national Computer Emergency Response Team (CERT) in cooperation with a foreign researcher, but it took weeks to be solved **(Cimpanu, 2019)**. Exposure of women's personal information is in itself a violation of their right to privacy, but it also makes women more susceptible to different types of online violence and harassment.

We do not yet have an agreed definition of the multiplicity of behaviors that constitute

[1] Although these numbers are estimates, as most countries do not submit gender disaggregated data to the International Telecommunication Union ITU (Web Foundation, 2018).

"online violence" against women, although it is commonly said to be the behaviors that target one specific woman. It may happen, for example, when a woman receives a direct message through the Internet or has her information disseminated over the Internet without her consent, potentially causing a range of negative and traumatic feelings **(PRC, 2018)**. Given the current importance of the topic and a growing demand for a legal and regulatory framework to more effectively address online violence against women, this White Paper aims to shed some light on the need for combating this violence. It briefly explains how women can be harassed online, and outlines some of the main problems in the public and private spheres. It also briefly reviews how these issues have been addressed in Latin American and Caribbean countries. Lastly, a toolkit provides practical steps that can be followed by women who wish to protect themselves from the risks of being exposed online.

Online Violence against Women

2

The 1994 Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women (Belém do Pará Convention), defines violence against women as "…any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere" (article 1).[2] When the Convention was written and adopted in the early 1990s, the "public sphere" did not include the online world. Society, however, has changed radically over the last 25 years and our online identities, activities and interactions are an increasingly important component of our public lives, especially for political figures, journalists and other people who live the majority of their lives in the public sphere. Our online activity has also contributed to blurring the line between the public and private spheres, to the extent that, for some, the distinction may no longer be useful.

The Inter-American human rights system has not yet established an agreed definition of the multiplicity of behaviors that constitute "online violence" against women within the framework of existing legal instruments such as the Belém do Pará Convention, and there is an urgent need to set these standards in order to provide a solid conceptual and normative basis for public policy and other actions that aim to address online violence against women.

In concrete terms, online violence occurs in different ways. It "may involve threatening or harassing emails, instant messages, or posting information online" **(PRC, 2018)** and "targets a specific person either by directly contacting them or by disseminating their personal information, causing them distress, fear, or anger" **(PRC, 2018)**. Equivalent terms that are used are "online harassment" and "cyber harassment". For the purposes of this paper, we have included any type of harassment or abuse under the broader term "online violence against women."

Pew Research Center (2017) outlines six different behaviors it classifies as "online harassment", namely "offensive name-calling"; "purposeful embarrassment"; "physical threats"; "sustained harassment"; "sexual harassment" and "stalking". **Citron (2014)** describes that "cyber harassment" "involves threats of violence, privacy invasions, reputation- harming lies, calls for strangers to physically harm victims, and technological attacks" (p.3). The consequences of such harassment range from mental distress,

[2] https://www.oas.org/en/mesecvi/convention.asp

damages in reputation and fear of real-world effects, and the problem is even more prevalent among women **(Pew Research Center, 2017 and INEGI, 2015).**

Social media can be used as a tool for harassment. A study conducted by **Amnesty International (2019)** has found that women are more likely to be harassed and abused on Twitter, with "direct or indirect threats of physical or sexual violence, discriminatory abuse targeting one or more aspects of a woman's identity, targeted harassment, and privacy violations such as doxing or sharing sexual or intimate images of a woman without her consent". While courts are still trying to understand the often subtle differences between free speech/protected speech and what constitutes a "true threat" **(Drake, 2015)**, many women are feeling unsafe online, and suffering violations of their human rights to live free of violence, to physical, mental and moral integrity, and to privacy.

The discriminatory abuse can be worse when the woman belongs to a vulnerable group such as indigenous population, is a person with a disability or any other intersectional identity. Further, considering the extent of information and data about ourselves available online, the amount of time we spend online, as well as the fact that we rely on the Internet for different types of social and professional interactions, the problem of harassment is becoming more prevalent than it has ever been, increasing the need for an immediate response that is legally solid and technically enforceable.

|a. What are some of the methods used for online violence?|

• **"Cyberbullying"** – The **Cyberbullying Research Center**, citing **Hinduja and Patchin (2014)** define it as "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices", highlighting its repetitive nature. **Ipsos (2018)** has found that awareness around the issue has been increasing in recent years. Nonetheless, adolescent girls are more likely to report being victims of cyberbullying than boys **(Patchin, 2016)**. Moreover, **Betts et. al (2017)** found a negative impact on how the value of learning is perceived among women that are subjected to bullying, which does not occur to the same degree among men. **Kwon et al (2019)** have found that being a victim of cyberbullying is co-related to having poor quality of sleep, leading to higher chances of depression among adolescents.

•**"Cyberstalking"**-Privacy Rights Clearinghouse explains that one type of online harassment is cyberstalking, which "involves using electronic means to stalk a victim, and generally refers to a pattern of threatening or malicious behaviors" **(PRC, 2018)**. There are varying definitions for the term, and in some cases the threat needs to be deemed credible, and in others an implied threat falls into the category **(PRC, 2018)**. It is relatively easy to stalk a person, given the fact that many have multiple social media accounts and a significant online presence. Further, many people are not fully aware of the privacy features provided by the platforms used.

•**"Cyber Mobs"** is a related concept and happens when online groups post offensive/ destructive content online, often competing with other groups with the intention of shaming someone **(Citron, 2014)**. An example of how this affects women is presented by **Coding Rights and InternetLab (2017)**, in which a Brazilian performer from the State of Bahia (northeast of Brazil) was leading an online contest when a cybermob was organized against her as a mass voting campaign for her competitor, leading to her getting the 2nd place at the contest.

•**"Doxing/Doxxing"**–"Dox" comes from "documents"/ ".doc" and doxing is the "unauthorized retrieving and publishing, often by hacking, of a person's personal information,

including, but not limited to, full names, addresses, phone numbers, emails, spouse and children's names, financial details" **(Women's Media Center, 2019)**. Amnesty International found in 2017 that one-fourth of women have been subjected to doxing at least once (Amnesty International, 2017).

•**"Identity Theft"** – Occurs when a person's personal data is used deceptively by another person **(Women's Media Center, 2019)**. For example, a Russian woman discovered her pictures were being used by another Twitter account that had become viral, and it took some time until she was able to fully recover her identity **(Kochetkova, 2016)**. Such identity theft might have both practical and psychological consequences that last for longer than one could imagine.

•**"Revenge Porn"/ "Non-consensual pornography"** – Is "the distribution of sexually graphic images of individuals without their consent" and this includes both images/ videos acquired with or without consent **(Netizens, 2019)**. Such scenarios are particularly harmful for women, given that their bodies and sexuality are subjected to cultural norms that are, in many cases misogynistic. A related concept is "sextorsion," where money or other demands are made in exchange for not disclosing pictures or videos with sexually explicit content. Considering that in some countries over 80% of adults have sent text messages with some type of sexually explicit content **(Stasko and Geller, 2015)**, many people are at risk for this type of online violence.

BOX #1 Deepfakes – A New Weapon Against Women

"Deepfakes" are videos that make use of machine learning techniques to switch one person's face onto another's **(Knight, 2019)**. Such technologies emerged in 2017 **(Deeptrace, 2019)** and are being used in different contexts, but the most common ones are related to politics and pornography. The number of deepfake videos online is growing exponentially and this is partially given the fact that it is now easier for non-experts to use certain technologies **(Deeptrace, 2019)**. The U.S. Department of Defense is even developing tools to automate forensic tools with the goal of catching deepfakes **(Knight, 2019)**.

According to **Deeptrace (2019)**, women are the main targets when deepfakes are used in pornography. Cases involving the use of such technology to attack women in politics are also starting to appear. One example is a well-known U.S. politician, who in 2019 appeared in a video as if she was drunk; the video quickly became viral on Facebook **(Rosenberg, 2019)**. This is particularly troubling given the fact that deepfakes are expected to seriously impact upcoming elections all over the world **(Parkin, 2019)**.

While all women are at risk of being harassed online, other aspects of identity – such as race, ethnicity, language, sexual orientation or gender identity, migrant status, and disability, among others – can compound the problem. Women who belong to diverse identities simultaneously are more vulnerable targets for online violence. As the Women's Media Center (2019) explains, a homosexual woman might experience homophobia, while a black woman can be a target of racism, in both cases while also being a target of sexism. This highlights the importance of looking at online violence against women from an inter-sectional perspective.

Women involved in political life are also frequently targeted by online harassers. The Organization of American States (OAS) adopted a Declaration on Political Harassment and Violence against Women in 2015, which recognizes the "structural factors that affect violence against women and socio-cultural and symbolic standards as well as social and cultural stereotypes that perpetuate it" (OAS, 2015). It encourages social networks, among other stakeholders, to adopt measures towards eliminating discrimination and sexist stereotypes (OAS, 2015). This is particularly important given the fact that political debates increasingly happen through social media platforms and many people now get their news on politics primarily through such platforms.

Through this overview it is possible to conclude that women are being targeted through various methods and technologies. A brief description on how some of these issues are addressed in Latin American and Caribbean countries is presented below.

How are these issues being addressed in Latin American and Caribbean countries?

3

Advancements have been seen in recent years across Latin American and Caribbean countries in combating online violence against women. Regarding legislation against "revenge porn", for example, Law# 13.772/2018[3] was enacted in December 2018 in Brazil, changing previous legislation in order to criminalize the non-authorized recording and exposure of nude or sexual contents. Such acts are now considered as "domestic violence" for the purpose of the Law in the cases in which there was a pre-existing relationship between the victim and the perpetrator. The media played a crucial role in fostering debate around revenge porn after concrete cases have occurred. Such debates led to legislative changes directly addressing the issue **(Neris et. al, 2018)**. Argentina, Chile, Mexico and Uruguay are examples of OAS member states that are currently discussing draft bills related to revenge porn **(Neris et. al, 2018)**. Mexico in particular has proposed a specific amendment to its Criminal Code and the General Law on Women's Access to a Life Free from Violence[4] that addresses cyber-harassment against women **(Cruz, 2019)**.

Further, various countries across Latin America have either passed legislation on political harassment against women (Bolivia), or are discussing related draft bills (Costa Rica, Ecuador, Honduras, México and Peru) **(OAS, 2017)**. According to what has been described above, this is important, among other reasons, because of the impact of technology on democratic debates.

In regards to police specialized in cybercrime and/or online violence against women, advancements have also been seen in recent years. Mexico has a division of its police service that is specifically focused on cybercrime, taking cases of online violence,[5] and an online governmental portal has contents specifically related to raising awareness of cyberbullying.[6] In Brazil, some states have specialized police departments, others do not.[7] In Peru, anyone can register a complaint of online violence through an online form, even if the person registering the complaint is not the victim.[8]

This is not an exhaustive review of what is happening in Latin American and Caribbean countries. Rather, it is a brief overview intended

[3] https://www2.camara.leg.br/legin/fed/lei/2018/lei-13772-19-dezembro-2018-787488-publicacaooriginal-157031-pl.html

[4] Ley General de Acceso de las Mujeres a una Vida Libre de Violencia

[5] http://www.ssp.df.gob.mx/ciberdelincuencia.html

[6] https://www.gob.mx/ciberbullying

[7] https://new.safernet.org.br/content/delegacias-cibercrimes

[8] http://www.noalacosovirtual.pe/

to demonstrate the complexity of the issue. It is possible to note that countries are moving towards recognizing and defining the problem, as well as strengthening protections for women online. At the same time, there are new methods and technologies appearing, and various forms of online violence are being put into practice every day.

With a view to contributing to the protections in place for women online, this White Paper concludes with a series of practical steps that can be taken by women, as well as useful resources that are available online.

Practical Steps that can be Taken Immediately

4

Starting with the practical steps outlined below is a good idea if you would like to protect yourself against online violence. Useful online contents you can look for can also be found below. Among these contents are guides and manuals that will help you further understand what online violence against women is and what measures can be taken against it.

|Preventive Measures:|

• **Use strong passwords and do not share them.** Make sure you have a strong password and that you keep it to yourself only. Moreover, do not repeat passwords across different platforms and services. For further information, check **OAS (2019)** "Password Do's and Don'ts" (p. 11).

• **Learn how to understand and change privacy settings of social media platforms.** Part of the information exposed online can be controlled through privacy settings. It is important to learn what the options are in terms of protecting your privacy. For example, it is important to keep posts private so that persons that are outside your network do not have access to the contents you post, and to use two-factor authentication to login. For further information, check **OAS (2019)** "Check Your Privacy Settings" (p. 09).

• **Use encrypted messaging apps for communicating.** Encrypted apps are a safer option, as it is harder for a person to access the contents that are exchanged through them. While regular cell phone text messages are not encrypted, apps such as Signal, Telegram, WhatsApp and Wire are.

• **Use a Virtual Private Network (VPN) to encrypt your online traffic.** This step is important especially when you are not using a private network (when you are accessing the Internet from a coffee shop or other public wireless network, for example). VPN services will allow your traffic to be encrypted so that other persons using the network cannot see what you are doing online. While most VPN services are not free, they are a good investment. For further information, check **OAS (2019)** "VPN Use" (p. 13).

If violence/ harassment/ threat / abuse occurs:

• **Keep the evidence of the violence/ harassment / threat / abuse.** Do not erase any evidence. It is crucial to keep any messages you have and any other form of evidence, such as screenshots that can be used to prove the violence/ harassment / threat/ abuse.

• **Report the violence to the online platform/service.** In most cases it is possible to report violence to the online platform/service itself. Report what has occurred immediately. The platform will investigate to determine if the contents exchanged violates existing "community standards," and may or may not take measures to remove the content and/or restrict the privileges and activity of the perpetrator. While each platform has its own rules, you can look for an example of how content removal and other aspects of rule enforcement are addressed by checking **OAS (2019)** "Enforcement of Our Rules" (p. 28).

• **Do not reply to any threatening/ harassing messages.** It is important not to "feed" the person who is perpetrating the violence. Do not reply to any messages that are intimidating/threatening. If possible, block the person so that messages can no longer be received. In most cases, the person you have blocked will not be notified if you blocked them.

• **Reach out to local authorities [This step should be taken with caution as only serious threats should be reported].** Besides the regular law enforcement authorities, there are specialized law enforcement authorities in many countries, such as police specialized in cybercrimes. Reach out to them or to any other local authorities that can provide help. In some cases, there are also police divisions specialized in violence against women, as well as online forms that can be used to register complaints of online violence.

• **Seek support from persons you trust and mental health professionals.** Being a victim of online violence is troubling and can deeply affect a person's mental health and well-being. It is important to have external support from professionals and persons you trust around you. They can help you in taking appropriate steps to address the problem.

• **Look for useful online resources.** There are manuals, toolkits and a wide range of online material that can be consulted. Some of these tools are listed below in **Section 5. "Useful Online Contents"**. Check, moreover, "Media Literacy and Digital Security" **(OAS, 2019)**.

Useful Online Contents

5

|Reports, Manuals and Toolkits|

• Media Literacy and Digital Security. Twitter Best Practices. OAS 2019
https://www.oas.org/en/sms/cicte/docs/20190913-DIGITAL-ENG-Alfabetismo-y-seguridad-digital-Twitter.pdf

• Acoso Online. Pornografia no consentida. Cinco claves para denunciar y resistir su publicación. 2017. (Spanish) Fundación Datos Protegidos; Equipo Latinoamérico de Justicia y Género (ELA); InternetLab; Hiperderecho; Acceso Libre; Ipandetec; Son Tus Datos; Fundación Datos Protegidos Bolivia; No! to Online Abuse and Harassment (NOAH); Fundación Karisma; TEDIC. https://acoso.online/cl/

• A First Look at Digital Security. Access Now. 2018. (English) https://www.accessnow.org/your-spring-welcoming-gift-is-here-the-freshest-version-of-a-first-look-at-digital-security/

• A toolkit for researching women's internet access and use. A4AI; World Wide Web Foundation, GSMA and APC. 2018. (English) https://webfoundation.org/research/a-toolkit-for-researching-womens-internet-access-and-use/

• Advancing Women's Rights Online: Gaps and Opportunities in Research and Advocacy. World Wide Web Foundation. 2018. (English) https://webfoundation.org/research/advancing-womens-rights-online-gaps-and-opportunities-in-research-and-advocacy/

• Online Harassment Field Manual. PEN America. 2019. (English)
https://onlineharassmentfieldmanual.pen.org/

• Manuals with a Gender Perspective. Tactical Tech. (English and Spanish) https://gendersec.tacticaltech.org/wiki/index.php/Manuals_with_a_gender_perspective

• Violencia Cibernetica. Lersy G. Boria Vizacarrondo. Procuradora de las Mujeres, Puerto Rico. (Spanish) http://www.mujer.pr.gov/Educaci%C3%B3nPrevenci%C3%B3n/Opusculos/Violencia%20Cibernetica.pdf

• Netizens Online Security Guide. 2019. (English)
https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view

• Safernet. Various contents related to cyber harassment (Portuguese) https://new.safernet.org.br/

|TEDTalks|

• How Online Abuse of Women Has Spiraled Out of Control. Ashley Judd. TEDTalk. 2016 (English).
https://www.ted.com/talks/ashley_judd_how_online_abuse_of_women_has_spiraled_out_of_control/transcript?language=en

• Anita Sarkeesian at TEDxWomen 2012. Anita Sarkeesian. 2012. (English)
https://www.youtube.com/watch?v=GZAxwsg9J9Q

• Grooming, el acoso ¿virtual?. Sebastián Bortnik. TEDxRíodelaPlata. 2016. (Spanish)
https://www.youtube.com/watch?v=0wZjKOulodo

|Documentaries|

• Netizens. Cynthia Lowen. 2019. (English) https://www.netizensfilm.com/

References

6

Amnesty International. (2017). Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet. Retrieved from https://www.amnesty.org/es/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Amnesty International. (2019). Why Twitter is a toxic place for women. Retrieved from https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

Betts, L. R., Spenser, K. A., & Gardner, S. E. (2017). Adolescents' Involvement in Cyber Bullying and Perceptions of School: The Importance of Perceived Peer Acceptance for Female Adolescents. Sex Roles, *77*(7), 471–481. https://doi.org/10.1007/s11199-017-0742-2

Cimpanu, C. (n.d.). Indian govt agency left details of millions of pregnant women exposed online. ZDNet. Retrieved from https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

Citron, D. K. (2014). Hate Crimes in Cyberspace. Harvard University Press.

Coding Rights, & InternetLab. (2017). Violências de gênero na Internet: Diagnóstico, soluções e desafios. Contribuição Conjunta Do Brasil Para A Relatora Especial Da ONU Sobre Violência Contra a Mulher. Retrieved from https://www.academia.edu/35642655/Viol%C3%AAncias_de_g%C3%AAnero_na_Internet_diagn%C3%B3stico_solu%C3%A7%C3%B5es_e_desafios

Comparitech. (2019). Cyberbullying Statistics and Facts for 2016—2019. Retrieved November 3, 2019, from Comparitech website: https://www.comparitech.com/internet-providers/cyberbullying-statistics/

Cruz, H. (2019). Proponen ley contra ciberacoso a la mujer. Retrieved November 12, 2019, from El Universal website: https://www.eluniversal.com.mx/metropoli/proponen-ley-contra-ciberacoso-la-mujer

Cyberbullying Research Center. (2014, December 23). What is Cyberbullying? Retrieved November 3, 2019, from Cyberbullying Research Center website: https://cyberbullying.org/what-is-cyberbullying

Deeptrace. (2019). The State of Deepfakes: Landscape, Threats and Impact. Retrieved from https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf

Drake, B. (n.d.). The darkest side of online harassment: Menacing behavior. Retrieved November 3, 2019, from Pew Research Center website: https://www.pewresearch.org/fact-tank/2015/06/01/the-darkest-side-of-online-harassment-menacing-behavior/

EQUALS. (n.d.). 10 Lessons Learnt: Closing the Gender Gap in Internet Access and Use Insights from the EQUALS Access Coalition. Retrieved from https://2b37021f-0f4a-4640-8352-0a3c1b7c2aab.filesusr.com/ugd/04bfff_33ded6f6855b4de5b7a09186e1c6add7.pdf

Franceschi-Bicchierai, L. (2017, September 21). This Ransomware Demands Nudes Instead of Bitcoin. Retrieved November 5, 2019, from Vice website: https://www.vice.com/en_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin

GSMA. (2015). Accelerating Digital Literacy: Empowering women to use the mobile internet.

Hinduja, S., & Patchin, J. W. (2014). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (Second edition). Thousand Oaks, California: Corwin.

INEGI. (2015). Módulo sobre Ciberacoso 2015 MOCIBA Documento metodológico. 20.

InternetLab. (2018). Como países enfrentam a disseminação não consentida de imagens íntimas? Retrieved November 4, 2019, from InternetLab website: http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/

Ipsos. (2018). Global Awareness of Cyberbullying Is Increasing, Though 1 in 4 Adults Haven't Heard of It. Retrieved from https://www.ipsos.com/en-us/news-polls/global-awareness-of-cyberbullying

ITU. (2019). ITU report on global digital connectivity finds gender digital gap is growing. Retrieved from http://digitalinclusionnewslog.itu.int/2019/11/05/itu-report-on-global-digital-connectivity-finds-gender-digital-gap-is-growing/

Judd, A. (2015). Forget Your Team: Your Online Violence Toward Girls and Women Is What Can Kiss My Ass. Mic. Retrieved from https://www.mic.com/articles/113226/forget-your-team-your-online-violence-toward-girls-and-women-is-what-can-kiss-my-ass

Knight, W. (2018). The Defense Department has produced the first tools for catching deepfakes. MIT Technology Review. Retrieved from https://www.technologyreview.com/s/611726/the-defense-department-has-produced-the-first-tools-for-catching-deepfakes/

Kochetkova, K. (n.d.). Um caso assustador de roubo de identidade no Twitter. Retrieved October 12, 2019, from https://www.kaspersky.com.br/blog/stolen-social-identity/5949/

Kwon, M., Seo, Y. S., Dickerson, S. S., Park, E., & Livingston, J. A. (2019). 0802 Cyber Victimization and Depressive Symptoms: A Mediation Model Involving Sleep Quality. Sleep, 42(Supplement_1), A322–A322. https://doi.org/10.1093/sleep/zsz067.800

Neris, N., Ruiz, J., & Valente, M. (2018). Enfrentando Disseminação Não Consentida de Imagens Íntimas: Uma análise comparada. Retrieved from InternetLab website: http://www.internetlab.org.br/wp-content/uploads/2018/05/Neris_Ruiz_e_Valente_Enfrentando1.pdf

Netizens. (2019). Netizens Online Security Guide. Retrieved from https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view?usp=embed_facebook

OAS. (2015). Declaration on Political Harassment and Violence Against Women. Retrieved from http://www.oas.org/en/cim/docs/DeclaracionViolenciaPolitica-EN.pdf

OAS. (2017). Fact Sheet—Violencia y acoso político contra las mujeres en el marco de la Convención de Belém do Pará. Retrieved from https://www.oas.org/en/cim/docs/ViolenciaPolitica-FactSheet-ES.pdf

OAS. (2019). Media Literacy and Digital Security: Twitter Best Practices. Retrieved from https://www.oas.org/en/sms/cicte/docs/20190913-DIGITAL-ENG-Alfabetismo-y-seguridad-digital-Twitter.pdf

Parkin, S. (2019). The rise of the deepfake and the threat to democracy. The Guardian. Retrieved from https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy

Patchin, J. W. (2016). 2016 Cyberbullying Data. Retrieved November 3, 2019, from Cyberbullying Research Center website: https://cyberbullying.org/2016-cyberbullying-data

Pew Research Center. (2017). Online Harassment 2017. Retrieved November 12, 2019, from https://www.pewinternet.org/wp-content/uploads/sites/9/2017/07/PI_2017.07.11_Online-Harassment_FINAL.pdf

PRC. (2018). Online Harassment & Cyberstalking. Retrieved November 5, 2019, from Privacy Rights Clearinghouse website: https://privacyrights.org/consumer-guides/online-harassment-cyberstalking

Rosenberg, A. (2019). Facebook exec's outrageous defense of the "drunk Pelosi" video doesn't add up. Retrieved from https://mashable.com/article/facebook-monika-bickert-drunk-pelosi-video/?europe=true

Stasko, E. C., & Geller, P. A. (2015). Reframing Sexting as a Positive Relationship Behavior: (528002015-001) [Data set]. https://doi.org/10.1037/e528002015-001

Unicef. (2017). Access to the Internet and Digital Literacy. Retrieved November 12, 2019, from https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_ACCESS.pdf

Web Foundation. (2018a). Advancing Women's Rights Online: Gaps and Opportunities in Research and Advocacy. Retrieved from http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf

Web Foundation. (2018b). Measuring the digital divide: Why we should be using a women-centered analysis. Retrieved from https://webfoundation.org/2018/05/measuring-the-digital-divide-why-we-should-be-using-a-women-centered-analysis/

Women's Media Center. (2019). Online Abuse 101—Women's Media Center. Retrieved November 3, 2019, from http://www.womensmediacenter.com/speech-project/online-abuse-101

World Bank. (2019). Population, female (% of total population) | Data. Retrieved October 12, 2019, from https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS

OAS More rights for more people

Canada

COMBATING ONLINE VIOLENCE AGAINST WOMEN

A CALL FOR PROTECTION

White paper series
issue 7

2019