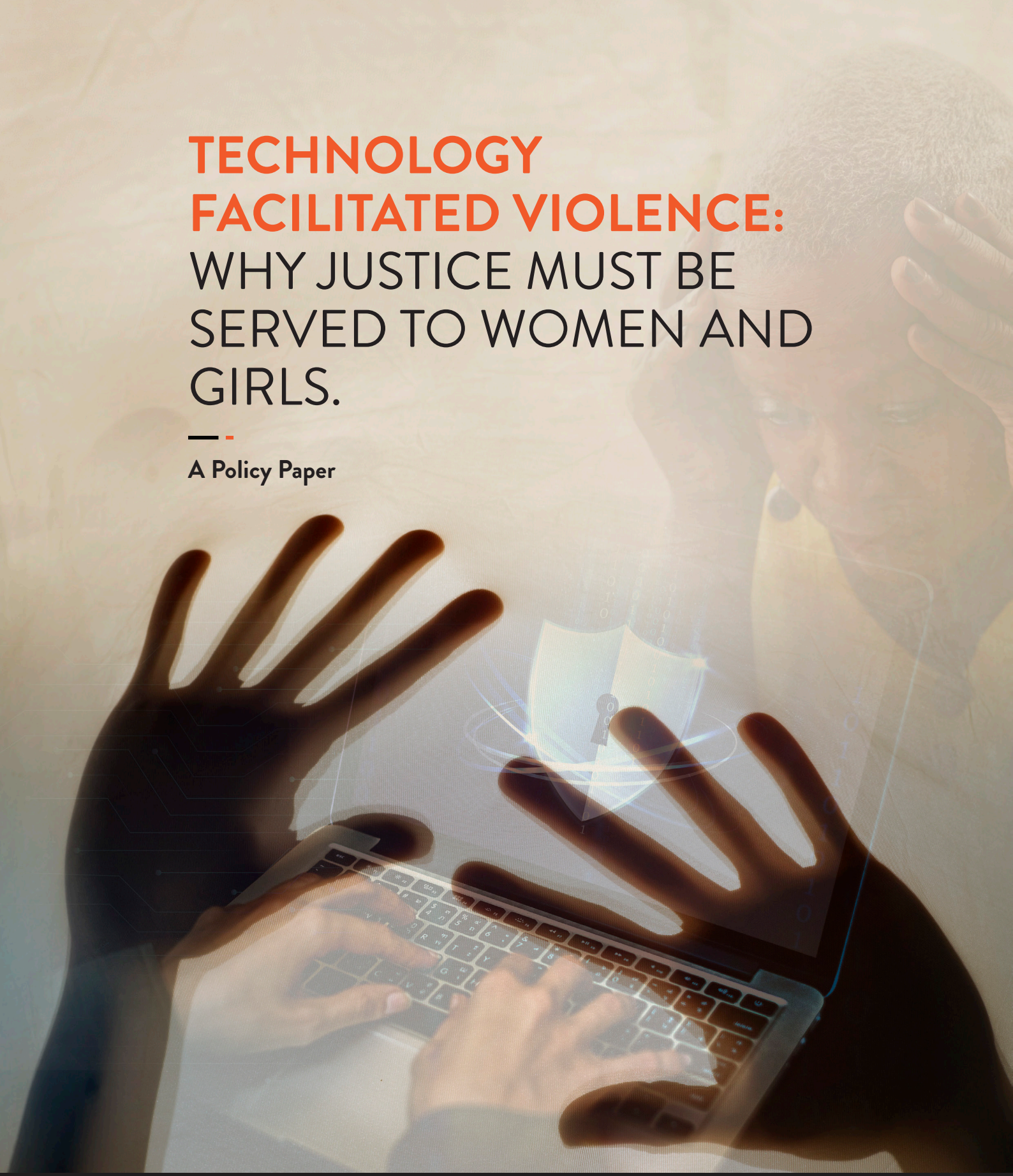
TECHNOLOGY FACILITATED VIOLENCE: WHY JUSTICE MUST BE SERVED TO WOMEN AND GIRLS.

A Policy Paper



UNWANTED WITNESS

"Amplifying Voices, Changing lives"

www.unwantedwitness.org

1.0 EXECUTIVE SUMMARY

We now live in a virtual society and physical violence which usually happens offline has extended to online and the internet makes it easier for people to commit violence without fear of any consequences for their actions. It is widely acknowledged that women and girls are the main targets of online violence, especially women with voices, like female journalists, activists and politicians.[1] Online harassment can include online bullying, trolling, cyber stalking, defamation and hate speech, public shaming, and identity theft and hacking, amongst other abuses.

This policy paper is informed by a research report by Unwanted Witness (UW) and partners, titled "**Weak Legal and Institutional Framework; A Hindrance to Justice for Survivors of Online Violence Against Women and Girls in Uganda**".[2] It argues that the internet mirrors and amplifies, in equal measure, the social norms of the offline world. It is argued that just as women and girls are exposed to risks of more types of violence than men and boys in the physical world, so too are they in the online world. As a result, abuse on digital platforms, especially when there are no apparent consequences for the perpetrators, may cause victims to opt-out of internet use and all the potential benefits that it affords.

It is argued that finding response strategies and solutions to the threat of cybercrime is a major challenge, especially for developing countries like Uganda. A comprehensive anti-cybercrime strategy generally contains technical protection measures, as well as legal and policy instruments. Technical protection measures are especially cost-intensive. Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlay on technical protection measures and network safeguards.

1.1 INTRODUCTION

Internet use is on the rise and social media platforms provide ever-increasing ways of staying connected. The future is certainly digital. 2019 was a landmark year because half of the world had begun to participate online, the 30th anniversary of the World Wide Web was celebrated; and it was estimated that there were 21.7 billion connected devices, with over 74,500 GB of data being sent over the internet every single second.[3] As of April 2020, there are 4.57 billion active internet users and 3.76 billion active social media users with the global online penetration rate being 59%.[4]

The onset of the COVID19 pandemic led to lockdown, school closures among other containment measures which put close to 700 million girls out of school. This means that more girls are spending more time than ever at home and on the internet and key societal functions are being moved online to prevent the spread of the virus, and it is more vital than ever that girls enjoy full and equal access to the opportunities social media and the web have to offer. This calls for the elimination or mitigation of instances of online violence against girls and women.

The term "cybercrime" is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime. One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences: Offences against the confidentiality, integrity and availability of computer data and systems; Computer-related offences; Content-related offences; and Copyright-related offences.

The **Broadband Commission** defines online violence against women and girls to include hate speech, hacking or intercepting private communications, identity theft, online stalking and uttering threats.[5]The Commission notes that it can entail convincing target to end their lives (counseling suicide or advocating genocide), as well as facilitating

1 https://www.unwomen.org/en/news/stories/2020/7/take-five-cecilia-mwende-maundu-online-violence
2 https://www.unwantedwitness.org/download/uploads/Weak-Legal-And-Institutional-Framework.pdf
3. Plan International (2020). State of the World's Girls Report : Free to be Online? Girls' and Young Women's Experiences of Online Harrassment.
4 The World Wide Web Foundation (2020).The online crisis facing women and girls threatens global progress on gender equality accessed at https://webfoundation.org/2020/03/the-online-crisisfacing-women-and-girls-threatens-global-progresson-gender-equality/ on 9 June 2021
5 The Broadband Commission (2019) State of Broadband Report 2019: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, accessed at https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf on 7 August 2021.

other forms of violence against girls and women including trafficking and the sex trade. It also includes activities such as trolling, cyber-bullying, e-bile, revenge porn and sexting.

The Sustainable Development Goals call for the use of ICT, including universal internet access, to tackle gender inequality. Mobile technology markets are expanding in developing countries, and there has been a rapid increase in access to the internet, but without robust measures to protect girls from online gender-based violence.

1.2 CONTEXTUAL ANALYSIS

In 2020, Plan International conducted the largest-ever global survey on online violence, which showed that 58 per cent of girls surveyed have experienced online harassment. One in five girls (19 percent) have left or significantly reduced their use of a social media platform after being harassed, while just over one in ten (12 percent) have changed the way they express themselves.[6]

A study by Unwanted Witness (UW) Uganda and partners on legal and institutional frameworks that can protect women and girls from online violence noted that 73% of women have encountered cyber violence, with women being 27 times more likely than men to be harassed online.[7] Furthermore, the report indicated that only 53% of the respondents indicated that they were aware that they can report cybercrimes and online violence.[8]

2.0 LEGAL AND POLICY REVIEW

The National ICT Policy 2014 talks about mainstreaming the issues of women, youth and persons with disabilities. "There is need to address them as special groups in society that can positively contribute to the growth of ICTs, as well as the use of ICTs as empowerment tools in their daily activities." As much as the policy acknowledges the need to mainstream the issues of women, it is silent about the issues regarding online violence against women and girls. Objective ix of the Policy to ensure that minors are protected from abuse such as pornography and violent programming. One of the strategies to achieve this objective is to establish and enforce ethical broadcasting standards that address both pornography and violence. This just puts into consideration the minors with no specificity to the women and girls.

Uganda has in place laws that attempt to address the issues regarding online violence against women and girls, however, there are gaps that need to be addressed in this framework.

2.1 The Constitution.

Article 21 of Uganda's 1995 Constitution states that all persons are equal before and under the law in all spheres of political, economic, social and cultural life and in every other respect and shall enjoy equal protection of the law.[9] The Constitution goes ahead to prohibit discrimination on the ground of sex, race, color, ethnic origin, tribe, birth, creed or religion, social or economic standing, political opinion or disability.

Article 33 of the Uganda Constitution explicitly states thus;
(1) Women shall be accorded full and equal dignity of the person with men.
(2) The State shall provide the facilities and opportunities necessary to enhance the welfare of women to enable them to realize their full potential and advancement.
(3) The State shall protect women and their rights, taking into account their unique status and natural maternal functions in society.
(4) Women shall have the right to equal treatment with men and that right shall include equal opportunities in political, economic and social activities.
(5) Without prejudice to article 32 of this Constitution, women shall have the right to affirmative action for the purpose of redressing the imbalances created by history, tradition or custom.
(6) Laws, cultures, customs or traditions which are against the dignity, welfare or interest of women or which undermine their status. are prohibited by this Constitution.

6 Plan International(2020). State of the World's Girls Report : Free to be Online? Girls' and Young Women's Experiences of Online Harrassment.
7 Unwanted Witness (2020). Weak Legal And Institutional Framework; A Hindrance To Justice For Survivors Of Online Violence Against Women And Girls In Uganda
8 Ibid
9 Refer to Article 21; Clauses 1&2 of the 1995 Uganda Constitution

2.1.1 Gap

Although the constitution in Article 21 provides legal protections to women and all Ugandans against discrimination and harassment, the constitution does not mention in any explicit way discrimination carried out via online and digital platforms leaving it to the interpretation of the lawyers and discretion of the judges.

2.1.2 Recommendation

An amendment of the Constitution to bring it in sync with the technological advancements made since it was promulgated in 1995 should be initiated. This can be through a Private Member's Bill moved by an individual Member of Parliament or lobbying in the Cabinet for a government-led constitutional amendment to include control of technology and digital spaces and address cyber-crime and online violence against women and girls.

2.2 Subsidiary Legislation

2.2.1 The Penal Code

Section 83 of the Penal Code23 Act observes threatening violence as an offence and the perpetrator is liable to imprisonment for a period not exceeding four years. The Penal Code Act further states that it is an offence to incite violence on the basis of, among other grounds, sex, traffic in obscene publications for the purpose of trade, cause another to die by suicide due to threats of violence, or attempt extortion by threats. Libel is also a crime in Uganda, and it applies to content which "exposes a person to hatred, contempt, or ridicule."

2.2.1.1 Gap

These offences do not target technology-related violence against women specifically, if the Penal Code is found to apply to online conduct, then threats, the non-consensual sharing of intimate images, or misogynistic speech against women, can be addressed under the Penal Code.

2.2.1.2 Recommendation

Amend the Penal code to explicitly provide for crimes related to online violence in line with regional and multilateral protocols, treaties and charters.

2.2.2 The Anti-Pornography Act 2014

The Anti-Pornography Act was put in place to define and create the offence of pornography; to provide for the prohibition of pornography; to establish the Pornography Control Committee and prescribe its functions, and for other related matters. Under the Anti-Pornography Act Section 13(1), it is an act of offence to produce, traffic in, publish, broadcast, procure, import, sell or abet any form of pornography.

2.2.2.1 Gap

The Anti- Pornography Act 2014 may discourage victims from reporting to the authorities for fear of retribution as Section 13 of the Anti- Pornography Act makes the victim and perpetrator equally liable under the law.

2.2.2.2 Recommendation

Amend and most preferably expunge Section 13 of the Anti Pornography Act because it creates double victimization of the victim which affects reporting and seeking redress after injustice has been meted out against the victim. The Act should be amended to provide more protection to the victim and more punishment to the perpetrator

2.2.3 The Computer Misuse Act 2011

The Computer Misuse Act (2011) is aimed at making provision for the safety and security of electronic transactions and information systems, to prevent unlawful access, abuse or misuse of information systems (including computers) and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters. The Computer Misuse Act (2011) prohibits cyber harassment, which is defined as using a computer to make "any request, suggestion or proposal which is obscene, lewd, lascivious or indecent" or to threaten to injure someone.

The 2011 Computer Misuse Act was enacted by the Parliament with the aim to, amongst other things, prevent unlawful access, abuse or misuse of computers. It provides definitions of cybercrimes, related penalties and some procedural measures that law enforcement authorities can use in their fight against cybercrimes. The Act specifies cybercrime in the following types which include, crimes that target computer systems, electronic fraud, and the production or distribution of child pornography.[10]

Any act of offensive communication is contrary

10 https://forensicsinstitute.org/cybercrime-in-uganda/

to section 25 of the Computer Misuse Act, which states that any person who willfully and repeatedly uses electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication, whether or not a conversation ensues, commits a misdemeanor and is liable on conviction to a fine not exceeding twenty-four currency points or imprisonment not exceeding one year, or both. The act states that any person who willfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyber stalking and is liable on conviction.

2.2.3.1 Gap

Definitions of obscene, lewd, lascivious, and indecent are not provided for in the Act which makes it hard to define the scope of crime.
Furthermore, "offensive communication" under the Computer Misuse Act is limited to electronic communication and may not cover the dissemination of pornography through other means.

2.2.3.2 RECOMMENDATIONS

An amendment of the Computer Misuse Act to provide definitions in its schedule to include "obscene, lewd, lascivious, and indecent" behavior online as well as expand the definition of "offensive communication" to include gender-based violence, harassment and threats of violence.

2.2.4 The Data Protection and Privacy Act 2019

The Data Protection Act was passed in 2019. The Act elaborates Article 27(1)(2) of the Constitution (1995) that guarantees the right to privacy. This act can be used to charge some of the cyber bullying tactics such as sharing of private conversations, private photos, and the collection of personal information without consent.

The Data Protection and Privacy Act (2019) aims at protecting the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information and for related matters.

2.2.4.1 Gap

The government has not yet established the office of the data protection commissioner which is essential for the full administration and implementation of the Act
Furthermore, the Ministry of ICT has not adopted and presented before Parliament the Ministerial Regulations that give effect to the Act. This makes its implementation ambiguous thus taking the sting out of the legislation.

2.3 POLICY PROPOSALS.

Given the strong importance international law and policy has on influencing public policy and domestic legal frameworks in member states, it is deemed necessary that activists, organizations and agencies should lobby the United Nations to come up with optional protocols to the 1) United Nations Convention on the Rights of the Child (UN CRC) and the Convention on the Elimination of All Forms of Violence Against Women (CEDAW). This is because the two human rights frameworks which provide protection to girls and women as well as safeguarding their basic rights and allowing for their participation in all aspects of their lives were drafted at a time when the online world did not exist.

The Ministry of Information and Communication Technology should be supported with finances and personnel to implement its proposed strategies to establish a national computer incident response team with a 24/7 call center, constituency computer incident response teams, a watch and alert center, and reporting mechanisms. The actualization of this plan will provide Uganda with a strategy within the government to ensure access and full-time availability of organized information and its integrity; keeping abreast with modern, safe and better technologies of information security by considering the trend of globalization; recognizing the contribution of the businesses and organizations in enhancing information security in addition to promoting information protection schemes and mechanisms for assurance.

CASE STUDY (GOOD PRACTICES): GERMANY'S LAWS ON PREVENTING ONLINE VIOLENCE

In 2017, the Federal Republic of Germany enacted the "NETzDG" Act to 'improve Enforcement of the law in Social Networks'.[11] The adoption of the legislation came at the heels of a fearsome spike in cases

11 Lam, A (2018). 87% of Germans Approve of Social Media Regulation Law accessed at https://daliaresearch.com/blog/blog-germans-approve-ofsocial-media-regulation-law/ on 8th August 2021

of online violence, harassment, fake news and hate speech. The law makes it a requirement for tech companies such as Facebook, Twitter, Reddit among others to remove abusive, offensive and other controversial content from their sites within 24 hours of posting.

The law places a fine of 50 million Euros on the companies for failure to remove harmful content on their sites. As a result of the law, Facebook has established two deletion centres in Germany with a 1200 strong workforce to monitor content.

In June 2020, the law was amended to require stronger accountability by social media companies and also criminal provisions for perpetrators.[12] The new amendments now bind social media companies – in addition to deleting posts within 24 hours – to report criminal content to the German Federal Criminal Police Office. It is an effective but controversial law that has come under much scrutiny on the basis that it restricts freedom of speech.

3.0 POLICY CHALLENGES.

It is difficult to quantify the impact of cybercrime on society on the basis of the number of offences carried out in a given time frame. Such data can in general be taken from crime statistics and surveys, but both these sources come with challenges when it comes to using them for formulating policy recommendations. Crime statistics can be used by academia and policy-makers as a basis for discussion and for the ensuing decision-making process. Furthermore, access to precise information on the true extent of cybercrime would enable law-enforcement agencies to improve anti-cybercrime strategies, deter potential attacks and enact more appropriate and effective legislation. Police records in Uganda do not have any complaints about computer crime and there are no other formal reports about cyber-crime rates in Uganda. Informal and scanty reports about computer crime in Africa and in Uganda particularly result in a misconception that those crimes do not feature there. This deprives decision makers, lawmakers and other stakeholders of the vital information that could be exploited for better planning and decision-making.

The restrictive policy terrain on various digital platforms is creating many pseudo users through the application of software like VPN. For instance, the ban on Facebook by the Ugandan Government is forcing citizens to use VPN in order to access it. This means that a VPN user in Uganda will be portrayed to have logged in from a far off country like Chile. This creates a lot of multi-territorial jurisdiction which makes the execution of internet protection laws and policies quite difficult.

4.0 CONCLUSION

In 2017, the Committee on the Elimination of Discrimination against Women (CEDAW) adopted a General Recommendation recognizing that gender-based violence happens in **'all spaces and spheres of human interaction', including 'technology-mediated environments, such as contemporary forms of violence occurring in the internet and digital spaces'**. It has been noted that most of the laws designed to regulate the internet are aimed at transactional, financial and e-commerce matters. Where laws do attempt to tackle harassment, many are outdated and ineffectual.

The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection. The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries. The development of technical measures to promote cyber-security and proper cybercrime legislation is vital for both developed countries and developing countries. Compared with the costs of grafting safeguards and protection measures onto computer networks at a later date, it is likely that initial measures taken right from the outset will be less expensive. Developing countries need to bring their anti-cybercrime strategies into line with international standards from the outset.

12 Oltermann (2018). Tough new German law puts tech firms and free speech in spotlight accessed at https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-andfree-speech-in-spotlight on 18 July 2021.

The Unwanted Witness
Bulange, Nsibambi Village P.O.BOX 23184 Kampala – Uganda
Mob: 697635 414-256+ **Email:** info@unwantedwitness.org