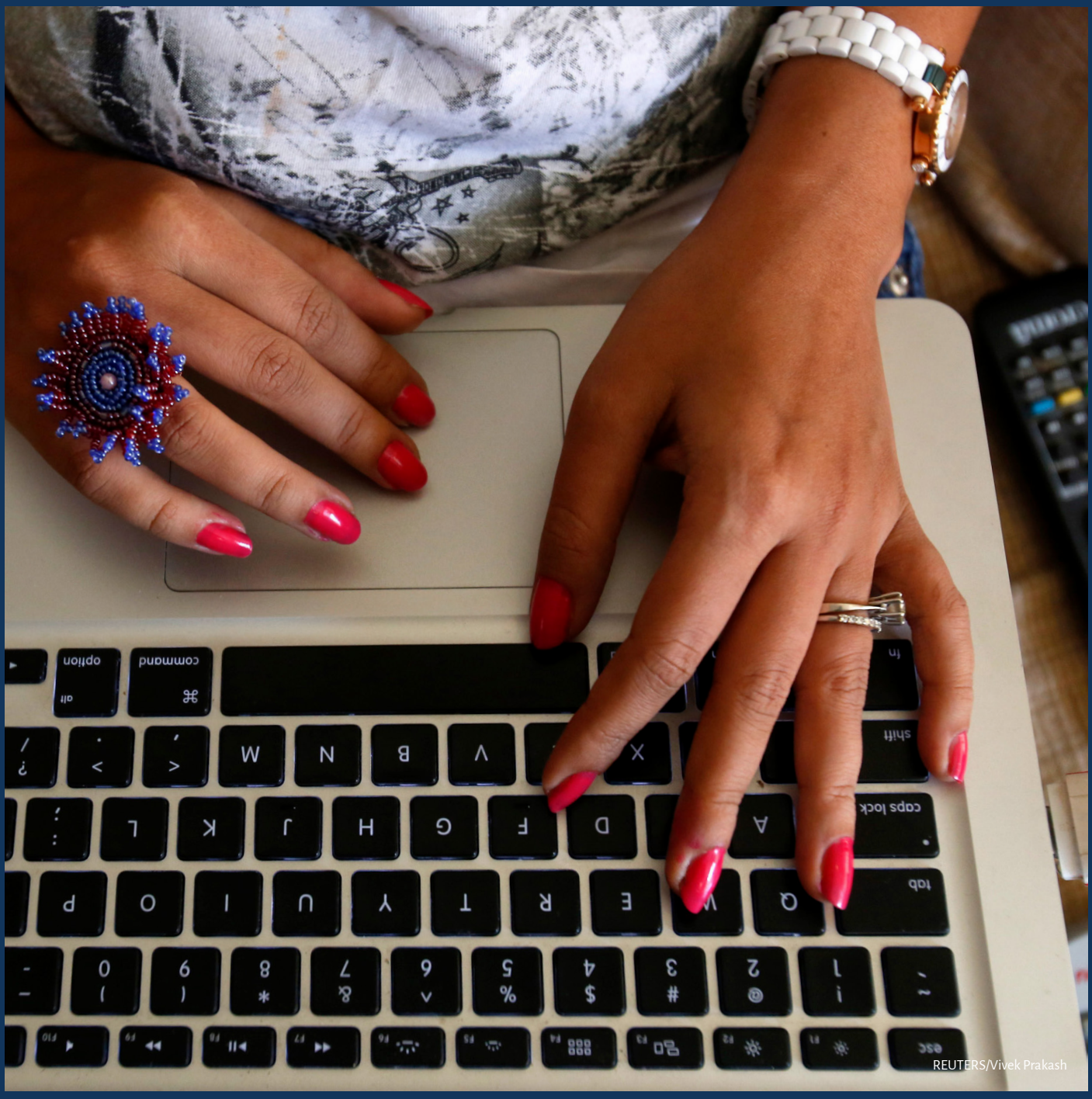


REUTERS/Vivek Prakash

Ending Online Sexual Exploitation and Abuse of Women and Girls:

A Call for International Standards

Equality Now
A just world for women and girls.

TrustLaw

THOMSON REUTERS FOUNDATION

ABOUT EQUALITY NOW

Founded in 1992, Equality Now is an international human rights organization that works to protect and promote the rights of all women and girls around the world. Our campaigns are centered on four program areas: Legal Equality, End Sexual Violence, End Harmful Practices, and End Sexual Exploitation, with a cross-cutting focus on the unique needs of adolescent girls. Equality Now combines grassroots activism with international, regional and national legal advocacy to achieve legal and systemic change to benefit all women and girls, and works to ensure that governments enact and enforce laws and policies that uphold their rights. Equality Now is a global organization with partners and members all around the world.

For more information, visit equalitynow.org.

facebook.com/equalitynoworg

@equalitynow

@equalitynoworg

ABOUT THE THOMSON REUTERS FOUNDATION

The Thomson Reuters Foundation is the corporate foundation of Thomson Reuters, the global news and information services company. The organization works to advance media freedom, raise awareness of human rights issues, and foster more inclusive economies. Through news, media development, free legal assistance, and convening initiatives, the Foundation combines its unique services to drive systemic change. Its mission is to inspire collective leadership, empowering people to shape free, fair, and informed societies.

THOMSON REUTERS FOUNDATION

ACKNOWLEDGEMENTS

This report is a publication by Equality Now, with design and publication support from the Thomson Reuters Foundation and Practical Law (Thomson Reuters). The report was made possible by the collective effort of many organizations and individuals. We acknowledge the contribution of TrustLaw, Thomson Reuters Foundation's global probono service, in coordinating the legal research on existing laws relating to online sexual exploitation and abuse at the international and regional levels, and the five countries covered in the report conducted by the following law firms: Aluko & Oyebode, Baker Botts LLP, Herbert Smith Freehills, Oduk – Ongati Advocates, and Shearman & Sterling. We appreciate Herbert Smith Freehills' work in reviewing the research and producing consolidated legal research which formed the foundation of this report.

We are also thankful to the following organizations who helped us connect with survivors and record their experiences: Africawide Movement for Children (Nigeria), Jan Sahas, Marie Collins Foundation, #MyImageMyChoice, NSPCC, and Trace Kenya. We are grateful to the activists and experts who generously contributed their expertise and perspectives, namely Dr. Debarati Halder, Mohamed Daghar, Ruchira Gupta, Sarah Kuponiyi, and Steve Grocki.

Finally, we are extremely thankful to the survivors for generously agreeing to share their stories in this report.

Disclaimer

This report is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances.

We intend the report's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. Equality Now, Aluko & Oyebode, Baker Botts LLP, Herbert Smith Freehills, Oduk – Ongati Advocates, Shearman & Sterling, the Thomson Reuters Foundation and Practical Law (Thomson Reuters), accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein.

Aluko & Oyebode, Baker Botts LLP, Herbert Smith Freehills, Oduk – Ongati Advocates, and Shearman & Sterling generously provided pro bono research to Equality Now. However, the contents of this report should not be taken to reflect the views of Aluko & Oyebode, Baker Botts LLP, Herbert Smith Freehills, Oduk – Ongati Advocates, and Shearman & Sterling or the lawyers who contributed.

Similarly, the Thomson Reuters Foundation is proud to support our TrustLaw member Equality Now with their work on this report, including with publication and the pro bono connection that made the legal research possible. However, in accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, we do not take a position on the contents of, or views expressed in, this report.

The Thomson Reuters Foundation, the Thomson Reuters Social Impact Institute, Equality Now, and all contributors to this report are committed to respecting human dignity and take reasonable measures to safeguard vulnerable persons. The photographs used in this report are for illustrative purposes only and are not intended to suggest that the subject(s) of those photographs are victims or perpetrators of online sexual exploitation and abuse.

TRIGGER WARNING: This report contains details from personal experiences of survivors of sexual exploitation and abuse as well as language from laws which refer to sexual violence and abuse, sometimes in explicit terms. We respect the lived reality and words of survivors, so we have not censored any language. However, we recognize that certain terms may be distressing for some readers. If you need support, please contact your local sexual violence center. You can also find resources and support information on page 69.

CONTENTS

ACRONYMS

AI	Artificial intelligence
AU	African Union
CDA	Communications Decency Act
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CPPA	Child Pornography Prevention Act
CRC	Convention on the Rights of the Child
CRC Guidelines	Guidelines regarding the implementation of the CRC Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
CRC Optional Protocol	Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
CSAM	Child sexual abuse material
DEVAW	United Nations Declaration on the Elimination of Violence against Women
EARN IT	Eliminating Abusive and Rampant Neglect of Interactive Technologies Act
EAW	European Arrest Warrant
EEA	European Economic Area
ESC	Electronic Service Communications
EU	European Union
EUROPOL	The European Union Agency for Law Enforcement Cooperation
FOSTA-SESTA	The Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ILO	International Labour Organization
INTERPOL	International Criminal Police Organization
Istanbul Convention	Convention on Preventing and Combating Violence against Women and Domestic Violence
IT	Information Technology
Lanzarote Convention	Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse
NCC	National Consumer Commission
NCMEC	National Center for Missing and Exploited Children
NDPR	Nigeria Data Protection Regulation
OAS	Organization of American States
OSEA	Online Sexual Exploitation and Abuse
POCSO	Protection of Children from Sexual Offences Act
SCA	Stored Communications Act
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
US	United States of America
Worst Forms of Child Labour Convention	International Labour Organization Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour
VDPA	Vienna Declaration and Programme of Action

Unsplash/Elly Brian

SETTING THE LANGUAGE

Words matter because they affect how we conceptualize issues, and they inform and shape our responses to the issues and actions to which they refer. Therefore, it is important to use the appropriate words when referring to OSEA. Below are definitions and descriptions of terms in this report and why we use them.

Adolescent girls: Although "adolescent" typically refers to people aged 10 to 19,[1] we use the term "adolescent girls" to describe females who are entering or have reached puberty and whose physical features are beginning to resemble those of adult females. We recognize that "adolescent girls experience higher rates of domestic and sexual violence[,] domestic servitude and exclusion from education, than adolescent boys".[2] Adolescent girls are particularly vulnerable to sexual exploitation and abuse. They experience multiple layers of discrimination: they are girls, they are young, and society sexualizes them.

Child: Refers to anyone aged under 18. This is based on the standard set by the UN Convention on the Rights of the Child.

Child sexual abuse material (CSAM): "CSAM" refers to visual material that depicts acts of sexual abuse and exploitation of children.[3]

Although many laws use the term "child pornography", it is increasingly understood to be inappropriate since it suggests a degree of consent on the part of the child. The term "child pornography" has also been criticized because pornography is increasingly being normalized which, according to the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), may contribute to trivializing and diminishing the seriousness of sexual exploitation and abuse of children.[4] According to the European Parliament, it is essential to use the correct terminology for the exploitation and abuse of children, "including the description of images of sexual

1 https://www.britannica.com/science/adolescence
2 UNICEF. Preventing violence and exploitation. https://www.unicef.org/bangladesh/en/raising-awareness-child-rights/preventing-violence-and-exploitation
3 ECPAT International (2017). Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection. https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf
4 ECPAT Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse available at http://luxembourgguidelines.org

abuse of children, and to use the appropriate term 'child sexual abuse material' rather than 'child pornography'."[5] "Child sexual abuse material" more appropriately describes the abuse and exploitation of children while protecting the dignity of victims.[6] Where the legal term "child pornography" is used, we will use the term "child sexual abuse material" instead.

Digital service provider and platform: "Digital service provider and platform" broadly refers to businesses providing services such as digital messaging and chat services, social media platforms, other internet-based services, and e-commerce services. This report will focus mainly on OSEA that occurs on these kinds of platforms.

Image-based sexual abuse: "Image-based sexual abuse" refers to the act of "having private, sexual images created and/or distributed without consent."[7] Although the term "revenge porn" is commonly used, we find it is inappropriate as it suggests it is pornography and not sexual abuse and suggests a degree of consent from the victim(s). The term "revenge porn" also implies the non-consensual sharing of nude or sexual images is the spiteful action of an ex-lover. In fact, research shows the motivations vary, including coercion in domestic violence situations, malice, bullying, and harassment.[8]

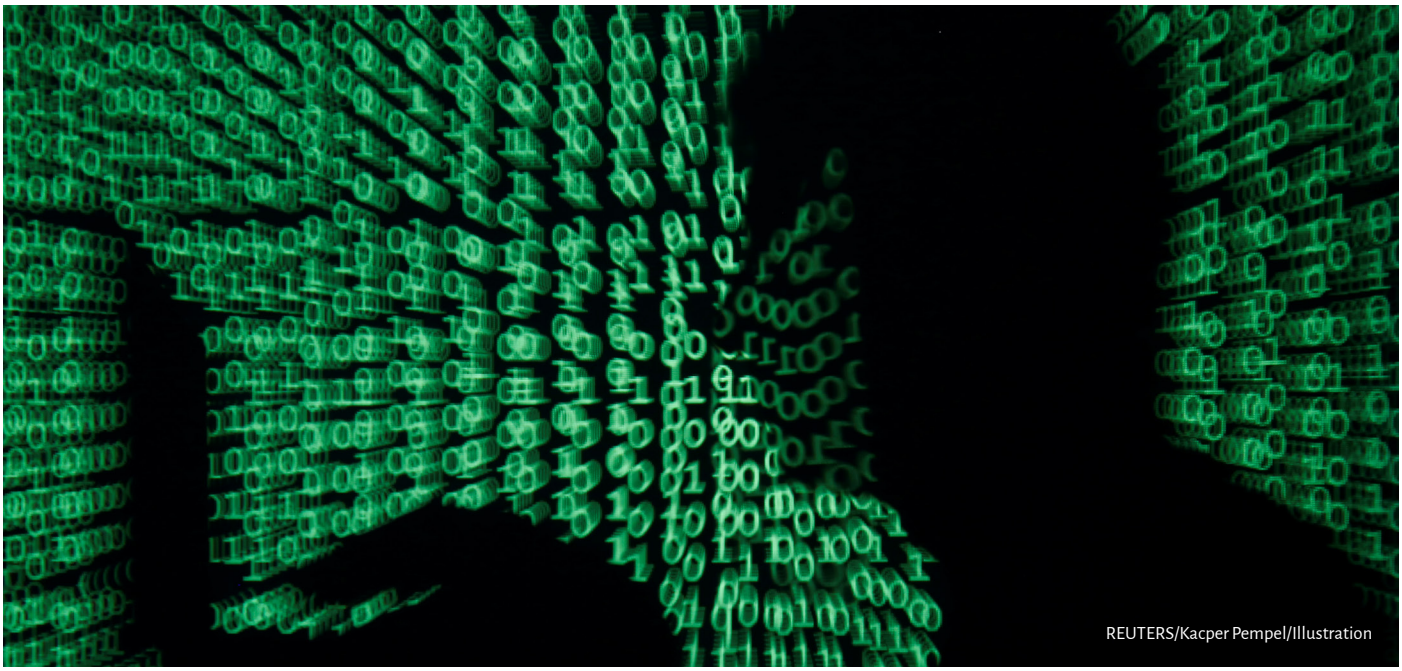
We will use "image-based sexual abuse" to include images and videos taken consensually but accessed without consent and then shared, as well as "locker-room" images and videos, recordings of sexual assaults arising from sexual coercion and extortion,[9] and images and videos produced through image manipulation such as deepfakes.[10]

Online sexual exploitation and abuse (OSEA): This term encompasses a number of sexually exploitative and harmful behaviors that occur or are facilitated online and through the use of digital technologies. OSEA includes online grooming, live-streaming of sexual abuse, CSAM, online sexual coercion and extortion, online sex trafficking, and image-based sexual abuse.

As technology evolves, new forms of abuse and exploitation emerge. Perpetrators often move victims from online spaces to in-person contact. When exploitation and abuse is only online, it is still traumatic. The impact on victims is not lessened.

Online sexual coercion and extortion: This term is the act of sharing (or threatening to share) sexual images or information online or through the use of digital technology as the means of coercion. The aim could be to cause distress to the victim, to gain financially, or to sexually abuse and/or exploit them. Other motivations may include malice or heightened attention on social media.

We use this term rather than "sextortion", which may not convey that the act involves sexual abuse and exploitation with extremely serious consequences for the victim.[11]



REUTERS/Kacper Pempel/Illustration

5 European Parliament. (2015) Resolution on Child Sexual Abuse Online. Doc. 2015/2564(RSP). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015IP0070

6 Internet Governance Forum. (2020). Glossary of Platform Law and Policy Terms. https://www.intgovforum.org/multilingual/filedepot_download/4905/2373

7 C. McGlynn, E. Rackley. (2017). More than 'Revenge Porn': Image-Based Sexual Abuse and the Reform of Irish Law. Irish Probation Journal Vol.14. https://www.pbni.org.uk/wp-content/uploads/2015/11/ClareMcGlynn_ErikaRackley_IPJ-13.11.17.pdf

8 C. McGlynn, E. Rackley. (2017). More than 'Revenge Porn': Image-Based Sexual Abuse and the Reform of Irish Law. Irish Probation Journal Vol.14. https://www.pbni.org.uk/wp-content/uploads/2015/11/ClareMcGlynn_ErikaRackley_IPJ-13.11.17.pdf

9 Ibid note 7

10 "Deepfakes" refers to artificially generated images depicting real people. Deepfakes use a form of artificial intelligence called deep learning to make images of fake events, hence the name deepfake

11 Please see https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation/online-sexual-coercion-and-extortion-of-children in the context of children


Unsplash/Rob Hampson

INTRODUCTION

"...the status of women will improve only with the elimination of the system that exploits them...."

Thomas Sankara[12]

INCREASED PREVALENCE OF ONLINE SEXUAL EXPLOITATION AND ABUSE (OSEA)

Sexual exploitation and abuse include many forms of coercive and predatory actions. The United Nations (UN) defines it as "any actual or attempted abuse of a position of vulnerability, differential power, or trust, for sexual purposes, including profiting monetarily, socially, or politically from the sexual exploitation of another."[13] Those who exploit others take advantage of the sex, gender, and structural discrimination inherent in our patriarchal society, and the economic inequality faced by women, children, and other vulnerable people for sexual gratification and, often, profit.

Digital technology and the internet provide significant opportunities for advancing gender equality and women's and children's empowerment, but ever-increasing internet and digital connectivity, camera-ready technology, and online anonymity are making it easier to groom, recruit, and sexually exploit with impunity. Anonymity and very limited regulation of online service providers and platforms also enable exploiters to easily contact potential victims.

Social media platforms and online gaming platforms are increasingly being used by predators to meet, groom, and abuse victims. With the widespread use of the internet, exacerbated during the COVID-19 pandemic, misogyny has found a new home, and old crimes of gender-based violence are taking new forms and being perpetrated online more easily.

OSEA is growing at an alarming pace globally. The full scale of the problem is not known because many cases go unreported due to victims blaming themselves and feeling shame, or being blamed and shamed by others, among other reasons. Victims may also fear prosecution or retribution from perpetrators or that the authorities will not take their reports seriously. This lack of reporting contributes to the vicious cycle of abuse. There are also gaps in monitoring. More attention is paid to monitoring online sexual abuse of younger children than of women, adolescents, and other groups.

12 I.A. Freeman. (2014). Seeds of Revolution: A Collection of Axioms, Passages, and Proverbs. (Vol.2) iUniverse.

13 UN (2017). Glossary on Sexual Exploitation and Abuse: Thematic Glossary of current terminology related to Sexual Exploitation and Abuse (SEA) in the context of the United Nations. https://hr.un.org/sites/hr.un.org/files/SEA%20Glossary%20%20%5BSecond%20Edition%20-%202017%5D%20-%20English_0.pdf

EFFORTS TO DETECT AND STOP OSEA

There is increasing public pressure on governments and digital service providers and platforms to act. However, measures to prevent and detect OSEA have been mostly left to digital service providers and platforms because of the different contractual, criminal, and private law[14] obligations placed on them in different countries. As a result, there has been heavy reliance on voluntary measures implemented by digital service providers and platforms.

The inadequacies of laws that specifically provide for OSEA and lack of clear definitions on what constitutes "harmful content",[15] as well as the reliance on community policing (i.e. relying on users to report harmful content and behavior), has resulted in inconsistencies in the application of the terms and conditions of use and standards of the service providers and platforms.[16] During 2018 it was reported that YouTube's "content moderation efforts have become more haphazard and inconsistent than ever".[17] Abusive material is not always removed online, particularly if it is not specifically classified as a crime in a specific country, or if the victim is not very obviously identifiable as a child (due to the emphasis and clarity on child protection). In addition, the tensions between freedom of expression and privacy and the right to protection and safety present challenges to efforts to prevent sexual abuse on the internet.

In this report, we examine whether legislative efforts are sufficient.

SCOPE OF THIS REPORT

This report considers what OSEA is and recognizes women and girls as particularly vulnerable. OSEA is part of the continuum of gender-based violence and is rooted in sex, gender, and intersecting inequalities and abuse of power that perpetuates women's and girls' subordination in society. We take a broad view of OSEA that includes online grooming, live-streaming of sexual abuse, CSAM, online sexual coercion and extortion, online sex trafficking, and image-based sexual abuse. We examine the law relating to these harms at the international level, at the regional level with a focus on Europe, as well as at the national level with a focus on Kenya, India, Nigeria, the United Kingdom (mainly England and Wales), and the United States. Although we aim to highlight the situation for women and girls, among the laws we explore are also those relating to children, on the understanding that many adolescents are legally children, and we examine the extent to which these laws protect them. In addition, abuse and exploitation that occurs during childhood often continues into adulthood. Children who have been abused are more vulnerable to being exploited and abused as adults.

The report also explores the relationship between aspects of digital rights – in particular privacy and freedom of expression – and protection and safety online. We consider how digital rights can be used to provide protection and recourse against OSEA and the tensions that arise when these rights are competing.

We also discuss the challenges posed by the multi-jurisdictional nature of online sexual harms and examine the challenges of regulating service providers and platforms. The testimony of survivors illustrates the impact of OSEA and highlights the challenges faced in keeping people safe and bringing perpetrators to justice. Finally, we provide recommendations targeted at governments, international bodies, and technology companies/ digital service providers and platforms.

...abuse and exploitation that occurs during childhood often continues into adulthood. Children who have been abused are more vulnerable to being exploited and abused as adults.

14 Private Law is a branch of the law that deals with the relations between individuals or institutions, rather than relations between these and the State

15 Institut Montaigne. (2019, June). Challenges of Content Moderation: Define "Harmful Content" - Interview with Claire Wardle. https://www.institutmontaigne.org/en/blog/challenges-content-moderation-define-harmful-content

16 S. Jhaver, S. Ghosha, A. Bruckman, E. Gilbert. (2018). Online Harassment and Content Moderation: The Case of Blocklists. ACM Transactions on Computer-Human Interaction 25(2):1-33. 10.1145/3185593

17 Wired. (2018, March). YouTube Doesn't Know Where Its Own Line Is. https://www.wired.com/story/youtube-content-moderation-inconsistent/

METHODOLOGY

This report examines laws relating to OSEA in international law and standards, in regional law and standards with a focus on Europe, and in five focus countries. We also highlight gaps and loopholes.

The misuse of digital technology and the internet to enable online sexual harms is a global problem, and the role of international law and standards to address it is critical. We aim to understand what protections exist and what opportunities there are for improvement.

Europe is a step ahead compared to other regions in terms of the laws and standards addressing OSEA. We explored these laws to see what lessons arise for the international community.

We selected five focus countries based on their regional diversity covering Africa, Asia, Europe, and North America: **Kenya** and **Nigeria** are two of Africa's leaders on internet uptake especially by young people; **India** is a growing technology hub; the **US** and the **UK** are key players in the fight against online child sexual abuse; and many of the digital service providers and platforms are domiciled in the US.

This report does not purport to be a definitive representation of all the relevant laws in any of the countries.

Notwithstanding, law firms provided pro-bono desk research in each of the countries, coordinated by TrustLaw, the Thomson Reuters Foundation's pro-bono service. As conducted, the research examined the following issues:

- Definitions of the term OSEA
- Laws addressing jurisdiction around OSEA crimes, and cooperation among states
- Laws concerning the right to freedom of expression or speech online and its relationship with OSEA
- Laws concerning the right to privacy online and its relationship with OSEA
- Laws concerning the regulation of digital service providers and platforms

Detailed profiles of each jurisdiction which contain excerpts from relevant legislation are provided in Annexes to this report.

Our partners helped us connect with survivors – children, adolescent girls and women who have experienced OSEA – whose stories are included in the report. Equality Now and our partners adhered to safeguarding policies in gathering the stories. We also feature expert testimony.

REUTERS/Brian Snyder


Unsplash/Towfiqu barbhuiya

EXECUTIVE SUMMARY AND KEY FINDINGS

Sexual exploitation and abuse include many forms of coercion and predatory actions. It is defined as any actual or attempted abuse of a position of vulnerability, differential power, or trust, for sexual purposes, including profiting monetarily, socially, or politically from the sexual exploitation or abuse of another. Online sexual exploitation and abuse (OSEA) encompasses several sexually exploitative and harmful behaviors that occur or are facilitated online and through the use of digital technologies. OSEA includes online grooming, live-streaming of sexual abuse, child sexual abuse material (CSAM), online sexual coercion and extortion, online sex trafficking, and image-based sexual abuse. Women and girls are particularly vulnerable as offenders take advantage of the sex, gender, and structural discrimination inherent in our patriarchal society, and the economic inequality that make them vulnerable to exploitation and abuse.

Technological advancements and the internet have also made it easier to groom, recruit and sexually exploit with impunity. Predators are increasingly using social media and online gaming platforms to target potential victims because these platforms offer anonymity and operate under very limited regulation. Consequently, OSEA is growing at an alarming pace globally, and the full breadth of the problem is largely unknown because of the large number of unreported cases.

This report:

- Evaluates OSEA as part of the continuum of gender-based violence against women and girls. We take a broad view of OSEA that includes online grooming, live-streaming of sexual abuse, CSAM, online sexual coercion and extortion, online sex-trafficking, and image-based sexual abuse.
- Examines the law surrounding OSEA at the international and regional level, with a focus on Europe. We also examine the laws surrounding OSEA at the national level, focusing on five countries, including Kenya, India, Nigeria, the United Kingdom (England and Wales) and the United States.
- Explores the balance between digital privacy, freedom of expression, and protection and online safety.
- Discusses the challenges posed by the multi-jurisdictional nature of online sexual harms and regulating service providers and platforms.

This report utilizes a survivor centric approach to illustrate the impact of OSEA and highlight the challenges faced in keeping people safe in a rapidly changing digital landscape.

OUR KEY FINDINGS

1 International and national laws have not kept pace with changing technology, and there is no single internationally binding instrument that specifically defines and addresses OSEA.

As technology continues to evolve at an alarming pace, so do the modalities of sexual exploitation and abuse. Yet, international and national legal instruments have simply not kept pace. Globally and nationally, there is a patchwork of laws that address different aspects of OSEA but do not adequately define OSEA or consider the technological aspects of OSEA. Current international and national laws that do address OSEA lack clear definitions of what constitutes "harmful content" and generally rely on community policing to identify perpetrators. Inconsistencies both internationally and nationally in the definitions of OSEA and the application of service providers' and platforms' terms and conditions for use have made it difficult to identify and prosecute perpetrators. Laws that do address OSEA often pre-date important technological advances, such as camera-ready technology, and do not adequately respond to the global and ever-evolving nature of the internet. Moreover, given that the internet is borderless, legal frameworks require a global scope to effectively address the problem. Global legal standards addressing OSEA must be created to provide standard definitions and laws for adoption both internationally and nationally.

2 The lack of consistent legislation and internationally adopted laws pertaining to OSEA make obtaining legal recourse extremely challenging.

Online criminal activities present challenges because they are rarely confined to one country or territory over which one legal system applies. In complex cases, there may be multiple offenders, multiple victims and multiple platforms, all based in different countries. This makes investigating and prosecuting OSEA crimes particularly challenging. Issues relate to which country has authority over the harm suffered, which country's laws will be applied to hold offenders accountable and which mechanisms will be applied to prosecute them.

While some international and national laws and mechanisms exist around establishing jurisdiction, many of them pre-date technological advances, and would require the various forms of OSEA to be clearly defined crimes at the national level and concerned countries to cooperate with each other to prosecute OSEA related crimes. International law and standards need to be updated to consider technological advances and the nature of international cooperation required for effective investigation and prosecution of these multi-jurisdictional crimes.

3 Inherent tension exists between digital rights and freedoms and the right to protection and safety against OSEA.

The mechanisms for balancing freedom of expression, privacy, safety, and protection from online harms provide some opportunities but are also fraught with many challenges. Freedom of expression and the right to privacy are fundamental rights for a well-functioning internet and any restrictions on these rights must be lawful and specifically tailored. Alongside the right to privacy and freedom of expression is the expectation that users are protected from harm. Tensions arise in practice at the intersection of these fundamental rights and expectations, and questions regarding how these rights should be balanced in law. One opportunity is the international law principle that in the event of a crime and/or human rights violation, privacy and freedom of expression of alleged offenders can be limited if the limitations are legal, legitimate, necessary, and proportional. The challenge is that there must first be adequate laws criminalizing OSEA and a globally accepted definition of what constitutes OSEA.

4 Regulations on digital service providers and platforms are inconsistent and often do not do enough to protect users against OSEA.

There is increasing public pressure on governments to ensure that user-generated content qualifying as OSEA does not appear on digital platforms and if it does that it is removed. However, measures to prevent and detect OSEA have been mostly left to self-regulation of digital service providers and platforms. Voluntary measures to address OSEA present many challenges, including a lack of precise rules and independent oversight, weak enforcement, and lack of sanctions. The inadequacies of laws to address OSEA, and lack of clear and consistent definitions of what constitutes "harmful content" has resulted in inconsistencies in the application of digital service providers and platforms terms and conditions of use and standards within and across countries. New international legal standards are needed that define the role, responsibility and accountability of digital service providers and platforms to address OSEA on their platforms.

KEY RECOMMENDATIONS

- The international community should adopt legally binding standards that:
  - clarify the role, responsibility and accountability of digital service providers and platforms in preventing, detecting, and reporting OSEA on their platforms;
  - clarify the interaction between protection and safety from exploitation and abuse and the rights of freedom of expression and privacy online; and
  - provide a framework to facilitate international cooperation to address OSEA that crosses multiple jurisdictions.
- The international community should review and update international and regional laws and instruments to ensure they are aligned to the reality of the digital age.
- Governments should enact and implement national laws and policies on OSEA that:
  - are aligned with global standards where they exist;
  - fully provide for protection of vulnerable people; and
  - account for the gendered and multi-jurisdictional nature of OSEA.
- Governments should have robust procedures to:
  - prevent OSEA;
  - implement laws to hold perpetrators to account; and
  - ensure victims are supported.
- Governments should ensure law enforcement agencies are fully aware of all forms of OSEA. There must also be enough capacity and expertise to investigate and prosecute alleged crimes effectively.
- Governments should enact and implement national laws that hold digital service providers accountable for OSEA on their platforms
- Digital service providers should apply a human rights approach in policies and practices to protect users from harm.
- Governments should have up-to-date information on national, regional, and international trends on OSEA so they can respond to emerging issues.

VICE/The Gender Spectrum Collection

Louise - UK
Survivor Story

I don't remember anyone speaking to me at school about online safety. The focus was on stranger danger, not about the guy on the internet. I was around nine when I first went on an online chatroom. You were supposed to be over 13 to join but I didn't have to give ID to prove my age. Men would message me and a lot would be very upfront, asking me to take my clothes off on camera. Every couple of weeks, I'd do what they asked if they were nice and I liked them. It's easy to manipulate a child, and getting attention from men made me feel grown up and validated.

When I was 12, I met a guy online who was 18, and it became a boyfriend-girlfriend thing although we never saw each other face-to-face. At the beginning, he'd say positive things like "I love you. You're my special girl. You don't have to go on camera if you don't want to." But then things started to shift.

We'd talk for hours, and he kept me isolated by saying, "You don't need friends; you have me." He'd ask me to touch myself, send videos, email him pictures, webcam stuff, and would get angry if I didn't. He tried to get me to send stuff every day, and there was standard emotional blackmail: "If you love me... nobody can find out, or we will get in trouble. Do you want me to be sent to prison?"

He'd tell me to stay up until 3 a.m., and I would force myself to stay awake because I'd worry I'd be in trouble. I didn't know what manipulation was at the time, but I was uncomfortable and could see he was being mean and twisting my words, so after three months, I ended things.

When I was 14, my family moved to a new area, and I went online to meet new people in chatrooms. I met a 34 year-old on TeenChat, and within a week, he'd driven two hours from where he lived to see me. I knew it was grooming, but I was lonely and vulnerable. It felt like our relationship was consensual. We'd speak every day, do stuff over Skype and the phone, and see each other at least once a month.

It lasted until I was turning 16 when it became obvious I was getting too old for him, and he was getting bored. We lost contact, and then a couple of years later, I got a call from the police. I remember instantly breaking down, admitting we'd had underage sex, and I had screenshots. It turned out that there were other victims, and he'd been doing it for a long time. He ended up being sent to prison for 15 years.

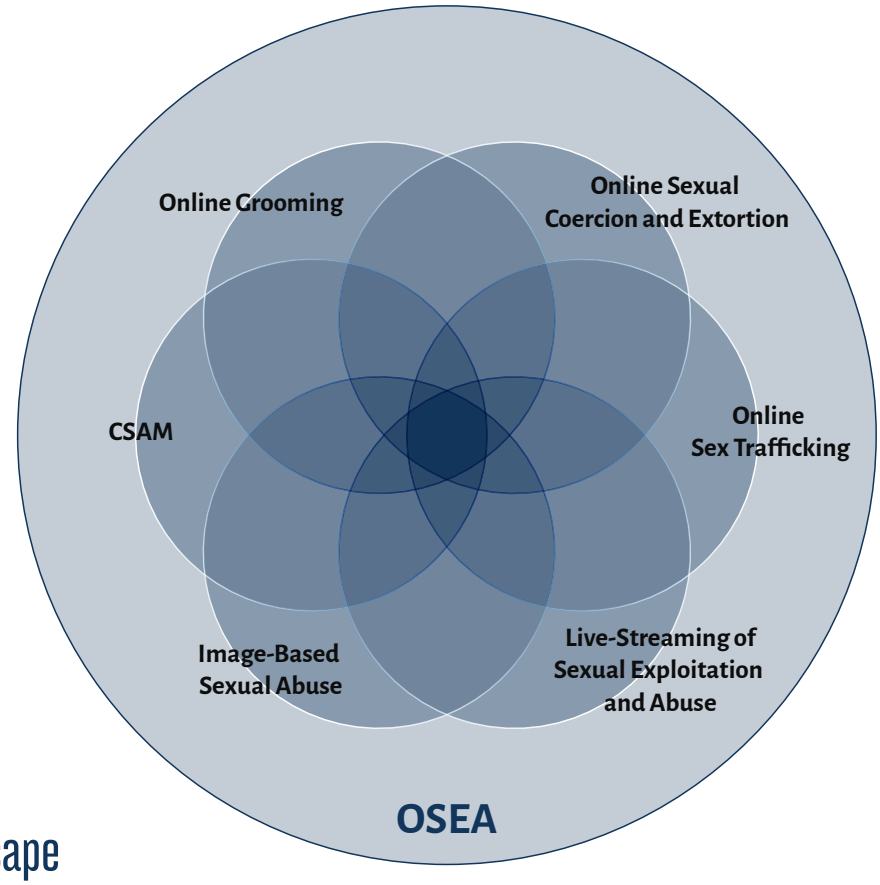
These things have affected my mental health, but it's got better since I was referred to a therapeutic counselling service by the NSPCC for children who have been sexually abused. I used to think guys accidentally went online and fell in love with me, that age is just a number, and it wasn't their fault. Now, I know what they were going online to look for, and I understand consent. But no matter how much help you have, what has happened will always have an impact.

"I don't remember anyone speaking to me at school about online safety. The focus was on stranger danger, not about the guy on the internet."

UNDERSTANDING OSEA

OSEA encompasses a number of sexually exploitative and harmful behaviors that occur online and can impact anyone - but particularly women and adolescent girls.[18] OSEA includes online grooming, live-streaming of sexual abuse, CSAM, online sexual coercion and extortion, online sex trafficking, and image-based sexual abuse. This list is not exhaustive, and as technology evolves new forms of abuse and exploitation emerge.

There is no single internationally binding instrument that specifically defines and addresses OSEA. Laws and standards differ across the world. Some of them address overarching issues of gender equality, violence against women and girls, and protection of children from sexual abuse which are connected to OSEA.



Understanding the Legal Landscape

International Law and Standards on Sexual Exploitation and Abuse

There are many international laws and standards that provide for governments to address sexual exploitation and abuse. While some consider the issue broadly to include women, girls, and children, others refer to specific forms of online abuse especially in relation to children, most prominently CSAM.

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the UN Convention against Transnational Organized Crime (Palermo Protocol),[19] which is one of the most ratified international instruments defines "exploitation" with regard to human trafficking to include: "the exploitation of the prostitution of others or other forms of sexual exploitation".[20] The UN Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) calls on States Parties[21] to address sexual exploitation of women in the context of trafficking and prostitution. In Article 6 it mandates States Parties "to take measures, including legislation to address all forms of traffic in women and exploitation of prostitution of women."[22]

Although non-binding, the UNHCR Sexual and Gender-Based Violence against Refugees, Returnees and Internally Displaced Persons: Guidelines for Prevention and Response (UNHCR Guidelines) define sexual exploitation as "any abuse of a position of vulnerability, differential power, or trust for sexual purposes; this includes profiting momentarily, socially or politically from the sexual exploitation of another."[23]

A number of international laws and standards focus on protection of children from sexual exploitation and abuse. For instance, the UN Convention on the Rights of the Child (CRC) in Article 34 calls on States Parties "to take all appropriate action at international, regional and national levels to protect children from all forms of sexual exploitation and abuse".[24] The CRC Optional Protocol[25] requires States Parties to protect the rights and interests of children from human trafficking and CSAM, among

There is no single internationally binding instrument that specifically defines and addresses OSEA.

18 National Center on Sexual Exploitation. https://endsexualexploitation.org/?eType=EmailBlastContent&eId=2676308c-3983-492d-aba3-e37d21d078d5
19 The Palermo Protocol was signed and ratified by the United Kingdom, the United States, all EU Member States, India and Nigeria. Kenya acceded to the Protocol.
20 Article 3 of the Palermo Protocol
21 States Parties refer to the nations that have signed onto a particular international or regional treaty. In some treaties they are referred to as Member States.
22 Article 6 of CEDAW
23 UNHCR. (2003). Sexual and Gender-Based Violence against Refugees, Returnees and Internally Displaced Persons. Guidelines for Prevention and Response. https://www.unhcr.org/uk/protection/women/3f696bcc4/sexual-gender-based-violence-against-refugees-returnees-internally-displaced.html
24 Convention on the Rights of the Child(1989). https://www.ohchr.org/en/professionalinterest/pages/crc.aspx
25 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography 2000. https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx

Laws Regulating Different Types of OSEA

Form of OSEA/ Country	Online Grooming	CSAM	Online Sex Trafficking	Live-Streaming of Sexual Exploitation and Abuse	Image-Based Sexual Abuse	Online Sexual Coercion and Extortion
International	There are gaps	Yes	Yes	There are gaps	There are gaps	There are gaps
Europe	There are gaps	Yes	Yes	Yes	There are gaps	There are gaps
India	No	Yes	There are gaps	No	There are gaps	There are gaps
Kenya	No	Yes	There are gaps	No	There are gaps	There are gaps
Nigeria	There are gaps	Yes	There are gaps	No	There are gaps	There are gaps
UK	Yes	Yes	There are gaps	There are gaps	There are gaps	There are gaps
US	Yes	Yes	There are gaps	There are gaps	Yes	There are gaps

Yes There are gaps No

others.[26] In addition, the UN Committee on the Rights of the Child more recently adopted General Comment 25 (2021) on children's rights in relation to the digital environment.[27] The General Comment clarifies that children enjoy the same rights in the digital space as they do in the physical space, and that their rights online are deserving of the same protection. The General Comment calls on States Parties to ensure these rights are protected, including the right to protection from online sexual crimes.[28]

The International Labour Organization Convention (ILO) Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (Worst Forms of Child Labour Convention) places an obligation on States Parties to design and implement programs and actions that eliminate the worst forms of child labor, which according to the Convention include the use, procuring, or offering of a child for prostitution, for the production of CSAM, or other sexually exploitative and abusive performances.[29]

There are also non-binding instruments adopted at the international level calling on countries to put in place measures to eradicate sexually exploitative acts against children, and the girl-child. For example, the Vienna Declaration and Programme of Action (VDPA) says the "exploitation and abuse of children should be actively combated, including by addressing their root causes".[30] The VDPA calls for effective measures against prostitution of children, CSAM, and other forms of sexual abuse. Similarly, the Yokohama Global Commitment[31] calls for timely implementation of legislation relating to the sexual exploitation of children and to undertake initiatives to combat the global trade in child sexual exploitation. The Yokohama Global Commitment was approved at the UN Second World Congress against Commercial Sexual Exploitation of Children. The Commitment notes the delegates' commitment to "take adequate measures to address negative aspects of new technologies" and mentions in particular CSAM on the internet.

International Law and Standards on Violence Against Women and Girls

The link between violence against women and girls, and sexual exploitation and abuse is clearly made in the Beijing Declaration and Platform for Action which sets out a framework for governments to take strategic action to address violence against women including sexual exploitation. The Platform for Action also calls on States to "eradicate violence against the girl child", by enacting and enforcing laws to protect children from all forms of violence including sexual exploitation, prostitution, and CSAM.[32]

The UN Declaration on the Elimination of Violence against Women (DEVAW) defines violence against women in Article 1 as "any act of gender-based violence 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 in private life." In its General Recommendation 19 (1992) on violence against women, the CEDAW Committee clarifies that discrimination against women, as defined in Article 1 of CEDAW, includes "violence which is directed against a woman because she is a woman or that affects women disproportionately" and that this violence constitutes a violation of their human rights. In addition, the Sustainable Development Goals, under Goal 5.2 call on governments to

26 Article 1 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
27 UN Committee on the Rights of the Child. General Comment 25. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?TreatyID=5&DocTypeID=11
28 UN Committee on the Rights of the Child General Comment 25
29 Article 3 of the International Labour Organization Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour
30 Article 48 of the Vienna Declaration and Programme of Action. https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx
31 UN High Commissioner for Refugees (UNHCR). (2001). Yokohama Global Commitment. https://www.refworld.org/docid/3f9fe2bd4.html
32 UNHCR. Strategic Objective L.7 of the Yokohama Global Commitment. https://www.un.org/en/events/pastevents/pdfs/Beijing_Declaration_and_Platform_for_Action.pdf

"eliminate all forms of violence against all women and girls in public and private spheres, including trafficking and sexual and other types of exploitation".[33]

The Council of Europe[34] has Conventions that relate to violence against women and children and various forms of sexual exploitation and abuse. These Conventions can be ratified by any country:

The Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) defines violence against women as, "all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life".[35] This provision can be interpreted to also apply to sexual violence and exploitation on the internet.

The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) criminalizes sexual offenses against children and defines sexual abuse as "engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities".[36] The prostitution of children is defined as "using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person".[37]

Regional Law and Standards

In the Americas, the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women (Belém do Pará Convention)[38] defines violence against women in Article 1 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." In Africa, Article 1j of the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol) defines violence against women as "all acts perpetrated against women which cause or could cause them physical, sexual, psychological, and economic harm". The Maputo Protocol makes reference to some aspects of OSEA by setting out an obligation for States Parties to take "effective legislative and administrative measures to prevent the exploitation and abuse of women in advertising and pornography".[39]

Across all focus countries, there are no laws that comprehensively address OSEA's different forms and impacts. Instead, different aspects of OSEA are provided for in different laws.

There are European Union (EU) Directives that provide for criminalization of some aspects of sexual exploitation. For instance, the Anti-Trafficking Directive 2011/36/EU[40] relates to the prevention and combating of human trafficking and protecting its victims provides that "exploitation shall include, as a minimum, the exploitation of the prostitution of others and other forms of sexual exploitation". In addition, the EU Combating Sexual Abuse of Children Directive[41] establishes minimum rules concerning the definition of criminal offenses and sanctions relating to sexual abuse and exploitation of children, more specifically on CSAM and solicitation of children for sexual purposes. The Directive specifically criminalizes the possession, acquisition, and distribution of CSAM.

Laws in Five Focus Countries

Similar to international provisions, there are no national laws in the focus countries that define or specifically relate to OSEA as a concept. However, Kenya, India, Nigeria, and the UK have ratified CEDAW and CRC, while the US has signed both treaties. All five focus countries have ratified the ILO Worst Forms of Labour Convention. The Palermo Protocol has been ratified by India, Nigeria, the UK, and the US, while Kenya has acceded to it. The CRC Optional Protocol has been ratified by India, Nigeria, the UK, and the US, and signed by Kenya. The UK has ratified the Lanzarote Convention and domesticated the EU Directives on human trafficking and child protection.

Across all focus countries, there are no laws that comprehensively address OSEA's different forms and impacts. Instead, different aspects of OSEA are provided for in different laws. In Kenya, there are laws[42] that address CSAM, as well as other forms of child sexual exploitation and abuse including the prostitution of children. The UK (specifically England and Wales and Northern Ireland) has applied existing criminal laws to the online context. For instance, image-based sexual abuse and CSAM can be

33 Target 5.2 of the Sustainable Development Goals. https://sdgs.un.org/goals
34 https://www.coe.int/en/web/about-us/our-member-states
35 Article 3(d) of the Istanbul Convention
36 Article 18 of the Lanzarote Convention
37 Article 19 of the Lanzarote Convention
38 32 out of 34 Member States of the OAS ratified the Convention. The US and Canada have not.
39 Article 13(m) of the Maputo Protocol
40 Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims. http://data.europa.eu/eli/dir/2011/36/o
41 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. http://data.europa.eu/eli/dir/2011/93/oj
42 See The Computer Misuse and Cybercrimes Act; The Children Act, The Sexual Offenses Act, The Employment Act

prosecuted under the "possession of extreme pornography"[43] provisions in the Criminal Justice and Immigration Act which set out what it means to be "in possession of", and the Criminal Justice and Courts Act which criminalizes image-based sexual abuse.[44]

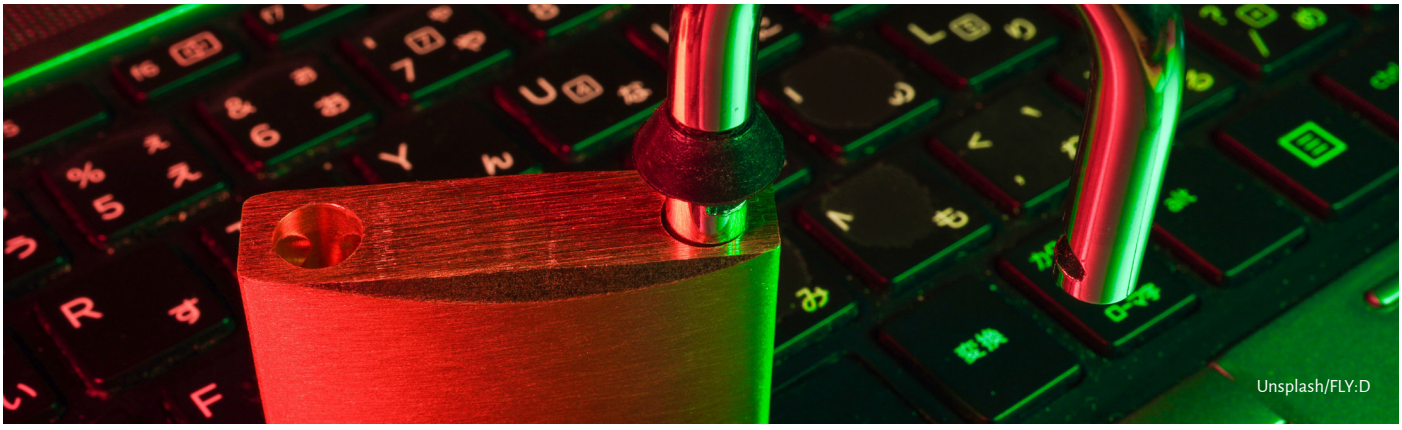
Similarly, Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act[45] criminalizes CSAM and in particular prohibits the use of any computer system or network to meet a child for the purpose of engaging in sexual activities with the child.[46] India takes a similar approach, and in its Penal Code,[47] provides for broad offenses that may be applied to OSEA. It defines "exploitation" as sexual exploitation of any form against adults or children.[48] The Penal Code also specifically makes it a crime to use obscene language,[49] insult women's modesty, or intrude on people's privacy.[50] Sharing sexual images online without consent and voyeurism[51] are also crimes. The Penal Code also makes it an offense to anonymously intimidate someone,[52] sexually harass someone,[53] or engage in digitally-enabled stalking.[54]

Conclusion

Most legislative instruments and standards were drafted with the understanding that sexual exploitation and abuse are perpetrated in the physical realm. OSEA is not specifically defined in international and regional instruments on violence against women and girls. Most of the instruments pre-date the realities and challenges that the digital age brings. Notwithstanding, a case can be made that these provisions are of broad application and can be interpreted as also applying to abuse that is happening or facilitated online. There is an argument that separating online and in-person sexual harms is a false dichotomy the two are interlinked as people experience their lives between online and physical spaces, and sexual predators recruit, groom, exploit and abuse their victims between the two spaces.

However, this approach does not always apply. Technological advancements present challenges that show legislative instruments and provisions are inadequate. Even where laws seek to address aspects of OSEA, they have not kept up with the ever-evolving nature of the problem. For instance, the CRC Optional Protocol does not criminalize live-streaming of child sexual abuse or online sexual grooming, which were not prevalent in 2000 when the CRC Optional Protocol was adopted. Another example is Article 23 of the Lanzarote Convention, which criminalizes online grooming only if there is an intention to "meet a child". It is no longer necessary for an offender to physically meet a child to commit a serious sexual offense.

In addition, while there is international recognition that sexual exploitation and abuse online and in-person impacts children, and other groups such as women and adolescent girls, there are no internationally binding instruments that are specifically targeted at OSEA affecting women. It is also not apparent in the child protection Conventions, because of their use of the general term "children", whether they were drafted with the particular needs of adolescents in mind as a specific demographic of children. The situation at the international level is reflected at the national level. Across the focus countries laws are more developed in relation to CSAM and child protection in general. Only the US, India, and the UK (England and Wales, and Northern Ireland) have obscenity statutes relating to abuse material depicting adults.


Unsplash/FLY:D

43 Section 63 of the Criminal Justice and Immigration Act 2008 (UK). https://www.legislation.gov.uk/ukpga/2008/4/section/63
44 Criminal Justice and Courts Act 2015 available at https://www.legislation.gov.uk/ukpga/2015/2/contents/enacted
45 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria). https://ictpolicyafrica.org/en/document/h52z5b28pjr?page=13
46 Section 23 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria)
47 Penal Code, 1860 (India). https://www.indiacode.nic.in/bitstream/123456789/4219/1/THE-INDIAN-PENAL-CODE-1860.pdf
48 Section 370(1) of the Penal Code, 1860 (India).
49 Sections 292 and 294 of the Penal Code, 1860 (India).
50 Section 509 of the Penal Code, 1860 (India).
51 Section 354C of the Penal Code (India).
52 Section 507 of the Penal Code (India).
53 Section 354A of the Penal Code (India).
54 Section 354D of the Penal Code (India).

Modupe - Nigeria
Survivor Story

I was 16 years old when I started accessing the internet. I had a friend who knew about things. She introduced me to Facebook and helped me create an account. As soon as I logged on I began receiving requests.

I didn't know the first person who contacted me. I started talking to him on Facebook and via webcam and soon we got very close. We were in contact for around three months and would communicate every day.

I don't know whether he lied to me about things like how old he was or what he did. I told him the truth about my own personal stuff so I didn't think he would lie. He would ask personal questions and I'd answer. I thought it was a way for us to get to know each other and feel comfortable with one another.

It went on like that for weeks until he said he wanted to see a picture and asked me to send something so I gave him ones of me wearing clothes. He said I should take the pictures not wearing anything, it would be better that way. I was lured into believing what we were doing was right and it was just this one person that I got close to like that.

I did what he asked and after a week or two I started seeing the photos with a few people, they were being passed around and shown to others. I had never met him face-to-face and I don't know where he lived but I began to wonder whether he was close by because soon everybody in my school and community knew - my parents, my friends, old or young, everyone.

When I started to see the photos around I felt very sad and depressed. People were always talking about the photos and saying stuff to me, bad stuff, it was very hard. Everybody wanted an explanation and they were always calling to hear from me. I had to pass by people who were talking about it, things got very bad and I was not sleeping.

I went to the police to report what had happened but I received no support. They asked me to show them the pictures and I just couldn't because I felt like I was the one publicizing them. The police started saying all sorts of things. They were ridiculing and laughing at me. I felt very bad about the way I was treated.

The police obviously don't know anything about online sexual exploitation. They have no education on the issue and took it lightly. They should have investigated the case and referred it to higher authorities that would be able to handle it better than they did. Instead, the person who did this to me has faced no consequences.

"I went to the police to report what had happened but I received no support. They asked me to show them the pictures and I just couldn't because I felt like I was the one publicizing them. The police started saying all sorts of things. They were ridiculing and laughing at me. I felt very bad about the way I was treated."


Unsplash/Emmanuel Ikwuegbu

Forms of OSEA

The most common forms of OSEA include online grooming, live-streaming of sexual exploitation and abuse, CSAM, online sexual coercion and extortion, online sex trafficking, and image-based sexual abuse. The forms of OSEA are distinct, but they are also connected. People from diverse backgrounds and geographical locations experience OSEA.[55] Women, adolescents (mainly girls),[56] and children are particularly vulnerable. In this section, we look at forms of OSEA, protection, gaps in protection, and opportunities for improving laws and standards.

Online Grooming and Solicitation for Sexual Exploitation and Abuse

Grooming occurs when someone builds a relationship with a person to manipulate, exploit and/or abuse them. The steps of grooming usually involve victim selection, gaining access to and isolating the victim. The person grooming is in a position of differential power over the victims and manipulates their position of vulnerability.[57] It is usually regarded as abuse that happens to children and/or young people, but vulnerable adults can also be affected.[58] Online grooming refers to grooming via the use of the internet and digital technology. Online grooming is usually perpetrated on social media platforms, dating apps, chatrooms, and gaming platforms. It can take place over a long period of time. It is important to acknowledge that grooming is a harm in itself.

International Law and Standards

At an international level, the existing laws provide for criminalization of online grooming only in relation to children as victims, leaving a gap in protection for vulnerable adults. The main legal instrument that could address online grooming is the CRC. Online grooming is ostensibly addressed by Article 34(a) of the CRC, which requires States Parties to criminalize "the inducement or coercion of a child to engage in any unlawful sexual activity." Moreover, the CRC Guidelines state that grooming and solicitation of children for sexual purposes "is a form of child sexual exploitation that may constitute an offense covered by the CRC Optional Protocol [on the sale of children, child prostitution and child pornography]."[59] Grooming is defined in the CRC Guidelines as "the process of establishing a relationship with a child either in person or through the use of ICT to facilitate online or offline sexual contact."[60] The CRC Guidelines also acknowledge the link between sexual extortion and grooming, and they recognize there is a developing trend towards "more extreme, violent, sadistic and degrading demands [being made] by offenders, which expose children to severe risks."[61]

The Lanzarote Convention, which is also exclusively focused on children, addresses online grooming in Article 23 where it provides that: "Each party shall take the necessary legislative or other measures to criminalize the intentional proposal, through information and communication technologies, of an adult to meet a child." Article 23 provides that the offense can only be committed by an adult. Article 23 also requires

55 Verham, Z. (2015) The Invisibility of Digital Sex Trafficking in Public Media. University of Virginia. Intersect, Vol 8, No 3.
56 See, https://www.theguardian.com/society/2020/oct/05/online-violence-against-women-flourishing-and-most-common-on-facebook-survey-finds. See also, https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html
57 https://www.mobieg.co.za/abuse/adult-grooming/
58 https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/
59 Guideline 68 of the UN Guidelines regarding the implementation of the CRC Optional Protocol. https://respect.international/wp-content/uploads/2020/01/Guidelines-Regarding-the-Implementation-of-the-Optional-Protocol-to-the-Convention-on-the-Rights-of-the-Child.pdf
60 Ibid. Note 55. at Guideline 68
61 Op. cit. Note 55 at Guideline 69

that the adult must have the intention to "meet a child." This is inconsistent with current thinking, given it is not necessary for an offender to meet a child in person to cause them sexual harm. The abuse can be through live-streaming, coerced taking and sharing of personal sexual images, or third-party activities.

European Law and Standards

European law also focuses on children. The EU Combatting Sexual Abuse of Children Directive[62] (Directive) establishes minimum rules concerning the definition of criminal offenses and sanctions regarding sexual abuse and sexual exploitation of children, CSAM, and solicitation of children for sexual purposes. It acknowledges that grooming and solicitation of children happens via information and communication technology through social networking websites and chat rooms.[63]

The Directive recognizes that the "solicitation of children for sexual purposes is a threat with specific characteristics in the context of the Internet, as the latter provides unprecedented anonymity to users because they are able to conceal their real identity and personal characteristics, such as their age."[64] In addition, Article 6 of the Directive mandates that Member States "take the necessary measures to ensure that an attempt, by means of information and communication technology, to commit the offences provided for in Article 5(2) and (3) [of CSAM] depicting that child is punishable."[65] The age of sexual consent varies across EU Member States (between 14 and 18 years). Children within the age of consent, as determined by the nation in question, who are solicited and groomed online may not be adequately protected, as they may be deemed to have consented. The Directive should be strengthened by defining a child as someone under 18. In the EU only Malta has identified 18 as the age of consent.

Laws in Five Focus Countries

Across the focus countries, online grooming is regarded as a crime against children.

Nigeria

In Nigeria, the Cybercrimes (Prohibition, Prevention, etc.) Act, Section 23 (3) criminalizes the act of intentionally proposing, grooming, or soliciting "through any computer system or network to meet a child for the purpose of engaging in sexual activities with the child." Similar to the Lanzarote Convention, the requirement of intent to meet the child for the purpose of engaging in sexual activities may make proving the offense more complicated. The law does not take into account the grooming that would have taken place before demonstration of the intention to meet the child, nor does it account for the fact that offenders do not have to meet a child in person to abuse them.

UK

In the UK, it is an offense under Section 15A of the Sexual Offences Act for a person aged 18 and above to communicate with a child for the purpose of obtaining sexual gratification or encouraging the child to "make a communication that is sexual." This provision may be applied to online offenses. However, similar to the Lanzarote Convention and the Nigerian Cybercrimes Act, liability requires proving that the adult established contact to meet the child for the purpose of committing a sexual offense against the child and took steps to physically meet the child.

US

In the US, it is a federal criminal offense to use mail or interstate commerce to entice a minor into sexual activity.[66] In practice, this law is commonly applied to prohibit online grooming of children, and offenders can be prosecuted for sexual grooming behavior as long as the activity crossed state lines for purposes of the interstate commerce requirement. Some US states have additional statutes providing for seducing a child online. For example, Florida[67]

Online grooming of children is generally prohibited under international, regional, and most national laws. However, a glaring gap at the international, regional and national levels is the failure of laws to recognize and provide for protection of adults who may also be vulnerable to online grooming.

62 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.
63 Recital 12 of the Directive
64 Recital 19 of the Directive
65 Article 6 of the Directive
66 Under 18 U.S.C. § 2422(b)
67 Florida Statute § 847.0135. http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899/0847/Sections/0847.0135.html

prohibits knowingly seducing or soliciting sexual conduct from a child online. Further, Illinois[68] prohibits knowingly using a computer online service, internet service, or any other device capable of electronic data storage or transmission for online sexual grooming.

Additionally, US federal law prohibits using an interactive computer service[69] to send a child any comment, request, suggestion, proposal, image, or other communication that is obscene or CSAM.[70] Although there are differences between states with respect to what qualifies as obscene material when a minor is involved,[71] courts lean toward protecting children from sexually exploitative behavior.

Unlike Nigeria and the UK, the US recognizes that grooming can take place without the offender physically meeting the child. Section 2422 of Title 18 of the US Code prohibits "anyone from knowingly persuading, inducing, enticing or coercing an individual to travel in interstate or foreign commerce with the purpose of engaging in prostitution or any criminal sexual activity, or attempting to do so." In ***US v. Chambers***,[72] the defendant was convicted of violating Section 2422. Chambers argued for reversal of his conviction because he neither intended to meet the minor child, who was in fact an FBI agent posing as a child, nor took a substantial step towards meeting her, despite chatting online with her for months. The Seventh Circuit held that Chambers had the requisite intent and had taken a substantial step toward meeting the minor, noting: "Child sexual abuse can be accomplished by several means and is often carried out through a period of grooming."[73]

Kenya

In Kenya, the Sexual Offences Act[74] takes a different approach and criminalizes displaying "obscene images, words, or sounds by means of print, audio-visual or any other media to a child" for the purposes of intending for the child to engage in a sexual act. This definition is not entirely satisfactory, as it requires that the display be of something "obscene." In reality, children may be groomed through "innocent" conversations.

India

Indian law recognizes that sexual abuse can take place in electronic form. Section 67B(c) of the Information Technology (IT) Act punishes the enticement of children to an online relationship with the purpose of publishing or transmitting material depicting children engaged in a sexually explicit act in electronic form.[75] In proving the crime, prosecutors must show harassment of the child, which includes "repeatedly or constantly follow[ing] or watch[ing] or contact[ing] a child either directly or through electronic, digital or any other means" with sexual intent.[76] In addition, the Home Ministry defines "cyber grooming" as "when a person builds an online relationship with a young person and tricks or pressures him/her into doing a sexual act."[77]

Conclusion

Online grooming of children is generally prohibited under international, regional, and most national laws. Where it is not specifically legally defined, prosecutors can often call upon other provisions relating to soliciting children. The challenge for conviction is often the requirement to show that the offender intended to meet the victim in person. The majority of existing laws do not take into account the evolving nature of online exploitation and the advent of camera-ready technology that makes it unnecessary for an offender to physically meet someone to abuse them. Some countries, such as the US, are paying attention to this inconsistency.

However, a glaring gap at the international, regional, and national levels is the failure of laws to recognize and provide for protection of adults who may also be vulnerable to online grooming. In addition, by failing to extend protections to exploited children once they become adults, the law fails to appreciate the long-term nature of online grooming.

68 Criminal Offences (720 ILCS 5/) Criminal Code of 2012. https://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=072000050HArt%2E+11+Subdiv%2E+25&ActID=1876&ChapterID=53&SeqStart=20300000&SeqEnd=21000000

69 Interactive computer service refers to any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions. https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=47-USC-1900800046-1237841278&term_occur=999&term_src=

70 18 U.S.C. § 1470.

71 The US Supreme Court has established a test which entails, among other things, assessing whether the average person, applying contemporary adult community standards, finds that the matter appeals to prurient interest or is offensive or lacks serious artistic, political, literary or scientific value. See *Miller v. California*, 413 U.S. 15, 15 (1973); *Roth v. United States*, 354 U.S. 476, 484–485 (1957); *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942). The test for what qualifies as "obscene material" involving minors is different, and the matter may be deemed obscene if it depicts a minor engaged in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, and the image lacks serious literary, artistic, political or scientific value. 18 U.S.C § 1446A.

72 642 F.3d 588, 592 (7th Cir. 2011).

73 (The court recognized that grooming refers to deliberate actions taken by a defendant to expose a child to sexual material. As a result, the court found significant evidence of grooming, which was sufficient to establish a violation of section § 2422(b): Chambers spoke to the minor in sexually explicit terms, e-mailed her adult and [CSAM], discussed sexual activities with her, instructed her on how to arouse herself, told her that he had sexual intercourse for years with his ex-girlfriend's 14-year-old daughter, and otherwise attempted to prepare her for a sexual encounter with him by discussing in graphic detail how the act would occur) See also *United States v. Berg*, 640 F.3d 239, 252 (7th Cir.2011) ("[Section 2422(b)] targets the sexual grooming of minors as well as the actual sexual exploitation of them. The statute's focus is on the intended effect on the minor rather than the defendant's intent to engage in sexual activity.").

74 Sexual Offences Act No. 3 of 2006, section 16 available at http://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/SexualOffencesAct_No30f2006.pdf

75 Section 67B(c), the IT Act.

76 Section 11 of the POCSO (the offense of committing sexual harassment upon a child), section 11(iv) (paragraph 3.1.3(F)) and 11(vi) (paragraph 3.1.3(D).

77 Learn about cybercrime, National Cyber Crime Reporting Portal, Ministry of Home Affairs. https://cybercrime.gov.in/Webform/CrimeCatDes.aspx

Cassie - UK
Survivor Story

We got our first computer when I was around ten. Chatrooms were a big thing. You'd get private messages from people you didn't know and have conversations. It didn't seem a big deal. We never had lessons about online safety, so we didn't know that people might not be who they say they are.

One afternoon when I was 13, I was online and started talking to someone who said she was a young woman. She was asking questions like: "How old are you? What music do you listen to? Do you get on with your dad? Where do you go to school?" I thought she was trying to make friends. It didn't seem like a barrage of questions.

It's normal for people to send photos to prove who they are so we sent ones of our faces. "She" said she was a model and that I could model too. She kept complimenting me, saying I was really pretty. It was flattering and the more she laid on the compliments, the more I got taken in.

She said she did topless modelling and asked me to send a topless picture. I didn't want to so she kept trying to convince me it was no big deal. Eventually I sent one. That was the turning point when she started blackmailing me, saying she would post my photo around my school and local area.

She said her boss wanted to meet me to take photographs for a model portfolio. She asked for my address. I was terrified and didn't feel like I had a choice. The following morning, a man came to my house and sexually assaulted me.

He was in his 50s, quite big and tall, a typical old man. He made me do things and took photos of everything. It went on for around an hour. I was only a young girl and didn't stand a chance. Even if I'd felt I was able to physically push him away, he said that he would make sure that all my family and school knew what had happened. That felt like the worst thing in the world.

After he left, the first thing I did was have a shower. I felt dirty, emotionally and physically, and wanted to wash everything off. I wasn't going to tell anyone and thought the police would say I was wasting their time.

I believed it was my fault. I had engaged with this person online, given my address, and opened the door. I was very angry and anxious.

Six months later, the police contacted me to say they'd found my details on someone's computer and wanted to make sure I was okay. It turned out this man had committed similar crimes.

He pleaded not guilty even though there was proof of him contacting young girls and photographic evidence of his crimes. The case went to court quickly because he was already under investigation. I was prepared to give evidence and be cross-examined. In the end I didn't have to testify, but even so, it was horrendous. In court, he had no remorse and sat there sneering. He got seven years for what he did to me, two years for two other victims, and two for a previous offense.

I was relieved I'd been believed and the court case hadn't been for nothing. I was also angry that it had happened to me, especially because he had a previous conviction and was able to commit similar crimes again.

The whole process ruined things for me for ten years. There was very poor support offered to me. The police did the standard thing of giving us some phone numbers, but nothing else was offered to me or to my family. Depression and anxiety lasted throughout my teens. I would have good and bad phases but continued to have panic attacks.

I didn't get counselling until I was 22. That's when I decided what had happened didn't have to define me. It really helped that I had a sense that justice had been done. Without that, it would have been more difficult for me to recover.

If you would like further information about Cassie's story, contact Marie Collins Foundation at info@mariecollinsfoundation.org.uk.

"I didn't get counselling until I was 22. That's when I decided what had happened didn't have to define me. It really helped that I had a sense that justice had been done. Without that, it would have been more difficult for me to recover."

Online Sexual Coercion and Extortion

Online sexual coercion and extortion refers to sexual exploitation and abuse when the means of coercion is abuse of power through threats or sharing sexual images or information online. Objectives can include causing distress to the victim, gaining financially, or sexually abusing them. Other motivations may include malice or social gains, such as popularity on social media. Online sexual coercion and extortion can result in CSAM, live-streaming of sexual abuse, image-based sexual abuse, and online sex trafficking.

International Law and Standards

Online sexual coercion and extortion is not provided for by any binding international instrument. It is addressed with a very narrow focus in the (non-binding) Combatting violence against women journalists report issued by the UN Special Rapporteur on violence against women.[78] Although the scope of the report is restricted, it is noteworthy in recognizing that the expansion of the internet is enabling new forms of online violence against women. The report mentions new forms of abuse, such as searching for or publishing someone's personal information with malicious intent, known as doxing, online sexual coercion and extortion, and image-based sexual abuse.[79] The report also considers the impact of online violence, noting "non-consensual distribution of intimate content [is] being used to defame and silence women journalists."[80]

European Law and Standards

It does not appear that Europe has any specific laws or standards that address online sexual coercion or extortion. That said, the right to be forgotten provided for in the EU General Data Protection Regulations (GDPR) offers some relief to victims of online sexual coercion and extortion.[81] This right, in theory, allows users to request that the digital service provider and platform remove content containing their personal data. This law might provide protection in that one might ask to be "forgotten" if the service provider hosted intimate content uploaded as a result of coercion and extortion.

Laws in Four Focus Countries

Across the focus countries, in the absence of specific online sexual coercion and extortion laws, there are avenues for prosecuting these cases under statutes that might not have originally contemplated this harm.

US

Under US federal law, the transmission, in interstate or foreign commerce, of any communication containing any threat to injure the property or reputation of the addressee or of another, is criminalized.[82] Prosecutors can use this law to pursue online sexual coercion and extortion cases.

UK

In the UK (England and Wales), prosecutors can use the general blackmail legislation in the form of the Theft Act, together with the Computer Misuse Act[83] to prosecute online sexual coercion and extortion. Under the Theft Act, it is a criminal offense to make any unwarranted "demand with menaces"[84] with a view to making gains or causing loss to another.[85] Furthermore, threatening to disclose an intimate image may be an offense under the Computer Misuse Act 1990 if the image is accessed via unauthorized use of a person's phone or computer.

Nigeria

In Nigeria, extortion is criminalized under the Criminal Code Law.[86] The provisions of the Code could be extended to cases of online sexual coercion and extortion if the crime fulfils the necessary elements - the main one being an intention to extort a person.

India

Sexual extortion and coercion are not specifically addressed by federal legislation in India. The closest provision is Section 503 of the Penal Code,[87] which defines criminal intimidation as when a person threatens injury to another (including their reputation) with an intent to cause alarm or to cause the victim to do or refrain from doing something.

Conclusion

Although it is accepted that this form of abuse is prevalent and impacts children, adolescent girls, women, and other vulnerable groups, there is a significant omission in laws that specifically address sexual coercion and extortion. The use of general extortion laws, Europe's "right to be forgotten," or the patchwork of laws in certain countries to combat sexual coercion and extortion is inadequate. The laws do not take into account that the offense is sexual.

78 UN. Human Rights Council. Special Rapporteur on Violence against Women. Combating violence against women journalists : report of the Special Rapporteur on Violence against Women, Its Causes and Consequences. https://digitallibrary.un.org/record/3865936?ln=fr
79 Paragraph 39 of the Combating Violence against Women Journalists Report.
80 Paragraph 42 of the Combating Violence against Women Journalists Report.
81 Article 17 of the GDPR available at CL2016R0679EN0000020.0001.3bi_cp 1..1 (europa.eu)
82 § 875(d) of Title 18 U.S.C (US)
83 Computer Misuse Act, 1990 (UK). https://www.legislation.gov.uk/ukpga/1990/18/contents
84 A "demand with menaces" refers to a high degree of coercion that includes threats of any action detrimental to or unpleasant to the person addressed. https://uk.practicallaw.thomsonreuters.com/w-007-7415?transitionType=Default&contextData=(sc.Default)&firstPage=true
85 Article 21 of the Theft Act, 1986 (UK). https://www.legislation.gov.uk/ukpga/1968/60
86 Section 408 of the Criminal Code Act 2004
87 The Indian Penal Code, available at https://legislative.gov.in/sites/default/files/A1860-45.pdf

Steve Grocki
Expert Interview - Part 1

Chief of the Criminal Division's
Child Exploitation & Obscenity Section,
US Department of Justice

The internet has many marketplaces where people can share child sexual abuse material (CSAM), as well as groom and solicit minor victims for sexual exploitation. In many instances, this illegal activity is happening in plain sight. Ongoing developments in technology, the move towards encryption, and widespread use of the Darkweb, are hindering identification and prosecution of crimes and we are seeing this across the spectrum. The technology is specifically designed to hide people's presence online and traditional forms of investigation are being thwarted.

It is very difficult for the global community to keep pace with the vast, complex and constantly evolving nature of the Internet, which is fundamentally global and borderless. There clearly has been an increase in the volume of CSAM online, particular the production of this type of content, which has increased three-fold between 2008 and 2019.

Apart from the biggest four or five companies, only a very small fraction of Internet companies voluntarily monitor their networks for CSAM and report illegal content involving children. Take a look at the App Stores or think of the number of websites out there, and quickly you'll see how many Internet companies there are. In the U.S., Internet companies have complete civil immunity and are insulated from civil liability even if they are knowledgeable CSAM being traded on their site. This insulation from liability provides them little incentive to spend limited resources and finances to develop robust online child safety practices.

Change needs to happen to improve online safety for children. There is lots of interest in the U.S., and we are working with foreign partners and Internet companies to institute a voluntary system outlining a baseline duty of care for child safety. In America, there is some appetite for legislative change (e.g. EARN IT Act of 2020) regarding civil liability for companies that are grossly negligent or reckless with child protection online. In other countries, regulatory schemes are also being discussed and considered.

There is clear evidence since the pandemic began - but also before it - of minors being enticed and groomed for self-production and other forms of child exploitation. It is a growing phenomenon and sextortion is a part of it. We see offenders targeting platforms that minors use and grooming children to self-produce content.

The biggest problem is that adults and children share platforms for online gaming, live streaming, or social media where is it quite difficult to know who is a child and who is an adult. It's a worrying trend.

We need to change the law to provide more privacy protection for CSAM victims, who can develop something akin to celebrity status within offender communities. If their true identities become known, they can be stalked and harassed many years after their abuse and childhood have ended. Offenders can post and trade information to identify the person, and we need to provide heightened protection to safeguard individuals' privacy before this can happen. Survivors already face the horror that recordings of their abuse continue to be circulated online and global law enforcement doesn't have the ability to remove it. Preventing harassment and stalking that can cause further harm is critical.

We get citizen reports about abuse content online. A lot of times, someone has come across something problematic and the platform isn't doing anything or is unaware of how its platform is being used to exploit children. These reports can be of great value because they signal where there are big problems and we can flag those issues to Internet companies, such as when platforms are being exploited by offenders, they aren't meeting reporting requirements, or when children under the age restriction are accessing inappropriate content.

TOR[88] and the Darkweb is what concerns me most because it enables offenders to exchange best practices with one another, to find out how others are succeeding, and teach one another. Offenders and potential perpetrators can find a community that normalizes a sexual interest in children. For someone new, it is like going to college, they can learn tricks of the trade without being identified, and this is a very scary development.

88 The Onion Router (TOR) is free and open-source software for enabling anonymous communication.

Child Sexual Abuse Material (CSAM)

CSAM refers to visual material that depicts acts of sexual abuse and exploitation of children whether virtually or otherwise.[89] Most countries have enacted legislation that addresses different aspects of CSAM.

International Law and Standards

Article 34 of the CRC mandates States Parties to take measures to protect children from all forms of sexual abuse and exploitation. Article 34 specifically prohibits "exploitative use of children in pornographic performances and materials." The CRC Optional Protocol highlights concerns about the growing availability of CSAM on the internet and other evolving technologies, and it calls on States Parties to prohibit its production, sale, consumption, and distribution. The CRC Optional Protocol highlights the need for international cooperation on this issue, and calls for approaches that address contributing factors, including gender discrimination, poverty, economic disparities, harmful traditional practices, armed conflicts, and trafficking in children.[90]

In addition, the ILO Worst Forms of Child Labour Convention requires States Parties to have in place measures to eliminate the worst forms of child labor, which according to the Convention, include "the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances."[91]

There are also a number of non-binding international instruments that call on governments to put in place measures to eradicate CSAM. These include the Vienna Declaration (the Declaration), which states "exploitation and abuse of children should be actively combated."[92] The Declaration also calls for governments to have effective measures against prostitution of children, CSAM, and other forms of sexual abuse. The Beijing Declaration and Platform for Action sets out a framework for participating governments to "eradicate violence against the girl child," by enacting and enforcing legislation protecting girls from all forms of violence including CSAM.[93] The Yokohama Global Commitment[94] calls for timely implementation of legislation relating to sexual exploitation of children and to undertake initiatives to combat the commercial sexual exploitation of children.

The Lanzarote Convention mandates that States Parties criminalize CSAM, which it defines as "any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes."[95] The Convention calls for other measures, such as training people who work with children, creating victim support programs, and encouraging people to report suspected abuse. The Convention calls for

Unsplash/Alexandru Acea

89 ECPAT 2017. Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection. https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf
90 CRC Optional Protocol. https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx
91 Article 3 of the International Labour Organization Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour
92 Article 48 of the Vienna Declaration
93 Strategic Objective L.7 of the Beijing Declaration and Platform for Action
94 https://www.mofa.go.jp/policy/human/child/congress01-y.html
95 Article 20 of the Lanzarote Convention

children to be protected in judicial proceedings, including concealment of their identity.

The Convention on Cybercrime of the Council of Europe (Budapest Convention) is the only binding international instrument on cybercrime. The US and UK have ratified the Budapest Convention. It serves as a guideline for any country developing comprehensive legislation against cybercrime and as a framework for international cooperation among States Parties to the Convention. Article 9 of the Convention mandates each Party to take measures to criminalize producing, offering, procuring, possessing, and distributing CSAM.[96] In terms of the Convention, CSAM depicts a child, someone who looks like a child, or realistic images depicting a child.[97] The protections mandated by the Budapest Convention are for persons under the age of 18. A State Party may, however, impose a lower age limit, which cannot be less than 16 years.[98] If States decide to lower the age-limit, older children would be left without protection.

European Law and Standards

The Combating Sexual Abuse of Children Directive addresses CSAM and prohibits the exhibition of CSAM through the use of technological means.[99] In particular, "acquisition or possession of [CSAM] shall be punishable by a maximum term of imprisonment of at least 1 year."[100] It prohibits the live exhibition of the abusive material through the use of "information and communication technology."[101] Furthermore, the Directive addresses "simulated sexually explicit conduct".[102] This means CSAM does not need to have been real to be outlawed by the Directive - it just needs to look real. Thus, deepfakes or other technologically generated material made to look like CSAM are covered by the Directive.

Laws in Five Focus Countries

UK

In the UK (England and Wales), CSAM offenses can be prosecuted under the Malicious Communications Act, which criminalizes the sending of communications "containing a message which is indecent or grossly offensive."[103] The Communications Act also criminalizes sending messages, images, and electronic communications that are partly or wholly indecent or grossly offensive.[104] Additionally, the Protection of Children Act[105] and the Criminal Justice Act[106] criminalize the possession, taking, distributing, advertising, or showing of indecent photographs or pseudo-photographs of a child.

US

In the US, the CSAM statutes[107] prohibit the possession, transportation, distribution, and production of CSAM. Furthermore, the US Code[108] also prohibits the sexual exploitation of children, and in particular, prohibits conduct involving the inducement, transport, or permitting a child to engage in sexually explicit conduct for the purposes of producing visual depiction, as well as the selling and buying of children.

India

In India, the Protection of Children from Sexual Offences (POCSO) Act provides for making, distributing, and possessing CSAM.[109] During 2020, new rules under the Act were implemented obligating digital service providers and platforms to report any information received relating to CSAM and provide law enforcement with any relevant material.[110] In addition, both the Information Technology Act and Penal Code make it an offense to distribute offensive material,[111] such as CSAM.[112]

Kenya

In Kenya, the Sexual Offences Act[113] provides for the most comprehensive provisions on CSAM by criminalizing the production, distribution, profiteering, and advertising of CSAM.[114] The Children Act,[115] although it does not explicitly provide for CSAM, lists subjection to sexual exploitation via CSAM as one of the criteria for determining if a child is in need of protection. In addition, the Computer Misuse and

96 Article 9 of the Budapest Convention available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
97 Article 9(2) of the Budapest Convention
98 Article 9 (3) of the Budapest Convention
99 Combating Sexual Abuse of Children Directive 2011/93/EU available at https://op.europa.eu/en/publication-detail/-/publication/d20901a4-66cd-439e-b15e-faeb92811424/language-en
100 Article 5(2) of the Combating Sexual Abuse of Children Directive 2011/93/EU
101 Article 2 of the Combating Sexual Abuse of Children Directive 2011/93/EU
102 Article 2(c) of the Combating Sexual Abuse of Children Directive 2011/93/EU
103 Section 1 of the Malicious Communications Act 1988 (UK). https://www.legislation.gov.uk/ukpga/1988/27/section/1
104 Section 368E(3) (za) of the Communications Act 2003 (UK). https://www.legislation.gov.uk/ukpga/2003/21/section/368E
105 Section 1 of the Protection of Children Act 1978 (UK). https://www.legislation.gov.uk/ukpga/1978/37
106 Section 160 of the Criminal Justice Act 1988 (UK). See also section 161 of the Criminal Justice Act 1988 which applies to Scotland. https://www.legislation.gov.uk/ukpga/1988/33/contents
107 Sections 2251-2260 of Title 18 United States Code
108 Section 2251 of Title 18 United States Code
109 Section 11, 13 and 15 of the Protection of Children from Sexual Offences Act, 2012 (India)
110 Bhandari, Vrinda & Kovacs, Anja (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. New Delhi, Internet Democracy Project. https://internetdemocracy.in/reports/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/
111 These provisions include section 67A paragraph 3.1.16, section 67B paragraph 3.1.14 and section 66E paragraph 3.1.18 of the Information Technology Act 2000 (India). https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
112 Bishaka Datta. (2017) Guavas and Genitals: A Research Study, in EROTICS South Asia Exploratory Research: Sex, Rights and the Internet. Association for Progressive Communications. https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf
113 Sexual Offences Act No. 3 of 2006, section 16 available at http://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/SexualOffencesAct_No3of2006.pdf
114 Section 16 of the Sexual Offences Act, 2006, Kenya
115 Children Act and the Sexual Offences Act (Kenya)

Cybercrimes Act can be interpreted to penalize behavior that constitutes CSAM. In particular, producing or possessing CSAM on or through a computer system or computer data storage medium is prohibited.[116] Other legislative provisions criminalize publicly exhibiting a visual, audio, or audio-visual media depicting a child.[117]

Nigeria

In Nigeria, the CyberCrimes (Prohibition, Prevention, etc.) Act establishes the crime of CSAM and prohibits producing, procuring, offering, distributing, possessing, and disseminating through the internet.[118] The Act also requires digital service providers and platforms to report CSAM on their platforms to law enforcement. It also includes grooming or soliciting a child for the purposes of engaging in sexual activities with a child or participating in sexually abusive performances with a child.

Conclusion

CSAM is extensively addressed by law internationally and nationally. However, there are some shortcomings. Definitions are not consistent across countries. For instance, countries have different laws on whether artificially generated images constitute CSAM. This is an area of growing concern with the advent of deepfakes. Among the focus countries, only the UK has specific provisions criminalizing the possession, procurement, production, and distribution of pseudo-photographs.

The detection of adolescent girls in CSAM on the internet is also a challenge for law enforcement and digital technology platforms. Human reviewers and automated tools that detect CSAM online cannot always be sure that images of girls who have reached puberty are not images of adults. The protection of adolescent girls in this regard requires specific attention in law.

Live-Streaming of Sexual Exploitation and Abuse

With live online streaming, non-consensual sex performances, sexual exploitation, and sexual abuse are simultaneously transmitted online and watched remotely. The abuse is achieved through coercion and extortion, force, manipulation, abuse of power, and/or grooming. It can also involve the use of technology to generate fake videos of real people, known as deepfakes.[119] Live-streaming is also a way in which CSAM and materials used for purposes of image-based sexual abuse are produced, as the recordings are sometimes stored and shared.

International Law and Standards

There are no international legal instruments that expressly refer to live-streaming of sexual exploitation and abuse. However, the CRC Guidelines acknowledge that technological developments have exposed children to new forms of sexual abuse, including live-streaming.[120] The CRC Guidelines recommended that Member States regularly revise legal frameworks to take into account technological developments and to ensure legislation provides for emerging forms of OSEA.[121]

As live-streaming does not require an offender to be in the same country as the victim, the CRC Guidelines advise governments to "enable the investigation and prosecution of such offenses regardless of the nationality or habitual residence of the alleged offender and victim".[122] Moreover, Article 34(a) of the CRC requires States Parties to take all the required measures to prevent "the inducement or coercion of a child to engage in any unlawful sexual activity". Article 34(a) could reasonably be construed to include online activity such as live-streaming of child sexual exploitation and abuse and online grooming.

The Lanzarote Convention requires States Parties to criminalize offenses that concern the participation of children in sex acts, including ones streamed online.[123]

European Law and Standards

EU law contains some specific provisions that relate to online streaming of sexual exploitation and abuse of children. In particular, the EU Combating Sexual Abuse of Children Directive refers to "pornographic performance" as a live exhibition aimed at an audience of a child's sexual organ or real or simulated sexually explicit conduct.[124]

Laws in Five Focus Countries

UK

In the UK (England and Wales), courts have considered cases involving the live-streaming of sexually exploitative material to fall within the "making" of an indecent image under the Protection of Children Act[125] and provisions in the Sexual Offences Act relating to child sexual offenses and abuse of a

116 Section 24 of the Computer Misuse and Cybercrimes Act 2018 (Kenya)
117 See section 15 of the Children Act and the Sexual Offences Act (Kenya)
118 Section 23 of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Nigeria).
119 See Deepfake videos: How and why they work — and what is at ...www.csoonline.com › Fraud › Security
120 Introduction (A)(2) of the Guidelines Regarding the Implementation of the CRC Optional Protocol. https://www.ohchr.org/Documents/HRBodies/CRC/CRC.C.156_OPSC%20Guidelines.pdf
121 Guideline 19 of the Guidelines Regarding the Implementation of the CRC Optional Protocol
122 Paragraph 87 of the UN CRC.
123 Article 21 of the Lanzarote Convention
124 Recital 8 of the EU Combating Sexual Abuse of Children Directive
125 Section 1 of the Protection of Children Act. Current prosecution guidelines follow *R v. Smith and Jayson* [2003] 1 Cr.App.R.13 in which the court stretched the definition of "make" by accepting the argument that causing an image to be shown on a computer screen constituted making it. This expanded definition is unlikely to deal with live-streaming in a satisfactory and permanent manner, as viewers of live-streaming would possess different criminal intent from makers of CSAM. Social Media - Guidelines on prosecuting cases involving communications sent via social media. https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media; Indecent and Prohibited Images of Children. https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children; Obscene Publications. https://www.cps.gov.uk/legal-guidance/obscene-publications.

position of trust.[126] Moreover, the Serious Crimes Act[127] may encompass live-streaming if a person views live-streamed sexual abuse, and there is evidence they encouraged the commission of a sexual offense.

In a 2019 case, which concerned the live-streaming of sexual abuse via Skype in exchange for payment,[128] one of the accused was prosecuted under section 72 of the Sexual Offences Act.[129] She was sentenced to 12 years and four months in prison. Another co-accused was convicted for making and distributing indecent images and conspiracy to sexually assault two children under the age of 13. He was imprisoned for eight years.

The UK has also successfully prosecuted nationals for watching videos of child abuse live-streamed from other countries. For example, in 2017, a UK court sentenced a national to 18 years in prison after paying £33,000 for more than 100 hours of footage of the abuse of 46 children in the Philippines. It took three years for the Philippine authorities to arrest those responsible for the abuse and identify and support some of the victims.[130]

US

In the US, the statute relating to CSAM, 18 U.S.C. § 2251, criminalizes coercing a minor to engage in sexually explicit conduct "for the purpose of transmitting a live visual depiction of such conduct".

Nigeria

Nigeria's Cybercrimes Act criminalizes recruiting, inducing, coercing, exposing, or causing a child to participate in sexual performances or profiting from or otherwise exploiting a child for such purposes. Further, it prohibits the use of any computer system or network for the production, provision, distribution, transmission, or procurement of CSAM,[131] which can be interpreted to also apply to cases of live-streaming.

Kenya

In Kenya, there is no explicit offense addressing live-streaming of sexual abuse. Instead, other legislation addressing CSAM is interpreted widely to penalize such behavior. In particular, the offense of producing or possessing CSAM on or through a computer system or computer data storage medium would cover live-streaming of sexual abuse.[132] Other legislative provisions provide protection for children from exposure to obscene materials and pornography.[133]

India

Similarly, in India, the IT Act makes it an offense to "transmit" offensive material.[134] These offenses can include the live-streaming of sexual abuse.

Conclusion

Although live-streaming of sexual abuse is not specifically provided for under international law, except in the CRC Guidelines, children can be protected by broadly interpreting provisions that provide for the distribution of CSAM and child sexual abuse. The CRC Guidelines provide protections for live-streaming of child sexual abuse and progressively acknowledge the impact of the internet on online child sexual exploitation and abuse in all forms. All legislative levels should similarly adopt laws that specifically penalize the live-streaming of sexual abuse of children and include broad protections able to cover new forms of child sexual abuse on the internet.

A gap in the law at all levels is the lack of specific protections for adults. In addition, a significant challenge for abuse involving adolescent girls is that the tools used to detect images and videos are not always able to determine the age of victims. This means older girls subject to abuse are likely to fall through the cracks. There are also no specific provisions to address the use of deepfakes in live-streaming.

Worryingly, in some countries, it is women and adolescent girls who are criminalized. In 2019, 10 women were arrested in Kenya and charged with trafficking obscene publications under Section 181 (1) (a) of the Penal Code.[135]

A gap in the law at all levels is the lack of specific protections for adults. This is a significant challenge for abuse involving adolescent girls as the tools used to detect images and videos are not always able to determine the age of victims. This means older girls subject to abuse are likely to fall through the cracks.

126 See Part 1 of the UK Sexual Offences Act, 2003
127 Serious Crimes Act 2015 (UK). https://www.legislation.gov.uk/ukpga/2015/9/contents/enacted
128 https://www.birminghammail.co.uk/news/midlands-news/woman-admits-being-paid-live-17228776
129 Section of the Sexual Offences Act, 2003 applies to British nationals committing offenses outside the UK
130 https://www.theguardian.com/global-development/2018/oct/08/british-paedophiles-target-children-poor-countries-online-abuse-national-crime-agency
131 Cybercrimes Act (Nigeria)
132 Section 24 of the Computer Misuse and Cybercrimes Act, 2018
133 See section 15 of the Children Act (UK) and the Sexual Offences Act (UK) which criminalizes publicly exhibiting a visual, audio or audio-visual media depicting a child.
134 These provisions include section 67A (paragraph 3.1.16), section 67B (paragraph 3.1.14) and section 66E (paragraph 3.1.18).
135 https://www.the-star.co.ke/counties/coast/2019-07-12-10-women-arrested-shooting-pornographic-film-dildos-recovered/

Sarah Cooper - US
Survivor Story

I was 12 or 13 when I first got a Facebook account. Early on, I would aimlessly go online once or twice a day for an hour or two. Things rapidly progressed and I joined various Facebook subgroups – music fan groups, ones about Harry Potter, Twilight, and animals. It was an outlet and way to meet like-minded people, where I felt like I could be myself without stepping outside of my comfort zone.

I wanted to be popular and initially it was about getting the largest number of friends on Facebook. I had multiple accounts and by 16, I had over 1,000 Facebook friends, many of whom were people I didn't know in person.

I didn't have a clue about the risks. Older men messaged me but I didn't want to connect the pieces, I wanted to be naïve. I honestly don't think it crossed my radar that people might be dangerous.

When I was 15, I got a Facebook request from a guy I didn't know. His profile picture was of a cartoon character and his username was "J". We started chatting and connected over music and books. Soon we were speaking all the time over Facebook Messenger, often late into the night. I told him all about my life, things in my past, problems I was having. We became really close and it felt like he adored me, like he was my best friend. He asked me to send some explicit photos and I did it because I wanted to be accepted by him. I was young and flattered by his attention and didn't realize that he was grooming me.

Things carried on for a few years, we started speaking on the phone but never saw each other in person. It was shortly after my 18th birthday that we finally arranged to meet. J pulled up in his car and I knew something wasn't right because I'd always thought he was around the same age as me but he looked closer to 40.

I wanted to sort things out so I went with him. He took me to a house where there were other people and they forced me to drink shots of alcohol and take cocaine. Then I was made to have sex with J and another woman. Someone else filmed it and they said it was my "audition" tape. I was terrified.

The next day J drove me to a motel. I was locked in a room guarded by armed men and sold into sexual slavery. There were other girls being held captive too and I thought I was never going to get out. When I begged to leave I was given drugs and alcohol that kept me in a daze. After a week and a half I managed to phone a friend, he drove to get me and we escaped.

For years, I didn't tell anyone what happened. I was scared but eventually, I thought enough is enough. There are so many stories of children being victimised, this stuff needs to be talked about, we need to get rid of the stigma. I'm sharing my story publicly because I don't want what happened to me to happen to anyone else. Internet safety education needs to be fully integrated into our children's curriculum. It's important to start talking about this stuff at a younger age, not wait until after young people are already experiencing this stuff.

Things could have gone a lot differently in my story if I had known more. I know it's not an easy conversation to have with a child, it's difficult and uncomfortable, but you need to speak with young people to make sure they have the knowledge to keep themselves safe.

"Internet safety education needs to be fully integrated into our children's curriculum... Things could have gone a lot differently in my story if I had known more. I know it's not an easy conversation to have with a child, it's difficult and uncomfortable, but you need to speak with young people to make sure they have the knowledge to keep themselves safe."

Online Sex Trafficking

Online sex trafficking refers to human trafficking for the purpose of sexual exploitation that is facilitated or perpetrated through the use of digital technology and the internet. Internet technologies are increasingly being used for the facilitation of trafficking. Some traffickers are taking advantage of digital platforms to advertise, recruit, and exploit victims.[136] Online sex trafficking includes recruitment of victims on social media and other online platforms, advertisement of sexually exploitative activities online with trafficked persons, and the use of video equipment to record, live-stream, and broadcast the exploitation of trafficked persons.

International Law and Standards

The Palermo Protocol is the most comprehensive international law on human trafficking and outlines the obligations of States Parties to address it. Article 3 defines human trafficking as the "recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion… to achieve the consent of a person having control over another person, for the purpose of exploitation." "The exploitation of the prostitution of others or other forms of sexual exploitation" is named as one of the forms of exploitation. Although it may be interpreted that the CRC Optional Protocol includes trafficking facilitated by or taking place online, the CRC Optional Protocol makes no specific reference to the use of technology and the internet to traffic and exploit.

CEDAW sets out the legal obligations of States Parties to "take all appropriate measures, including legislation, to suppress all forms of traffic in women and exploitation of prostitution of women".[137] In 2020, the CEDAW Committee adopted General Recommendation 38 on trafficking in women and girls in the context of global migration.[138] This Recommendation recognizes the challenges that the use of digital technology and the internet present for trafficking of women and girls, and makes a number of recommendations that governments and technology companies can implement to address the problem. Among them, the Recommendation calls on governments to "initiate proactive identification of production of online sexual abuse material during the COVID-19 and afterwards."[139] It also calls for collaboration between governments and digital service providers and platforms in law enforcement efforts such as information sharing in criminal investigations and identification of offenders.[140]

The CRC Committee made similar recommendations in General Comment 25 (2021) on the rights of children in the digital environment specifically recommends that States Parties "..should develop and update anti-trafficking legislation so that it prohibits the technology-facilitated recruitment of children by criminal groups."[141]

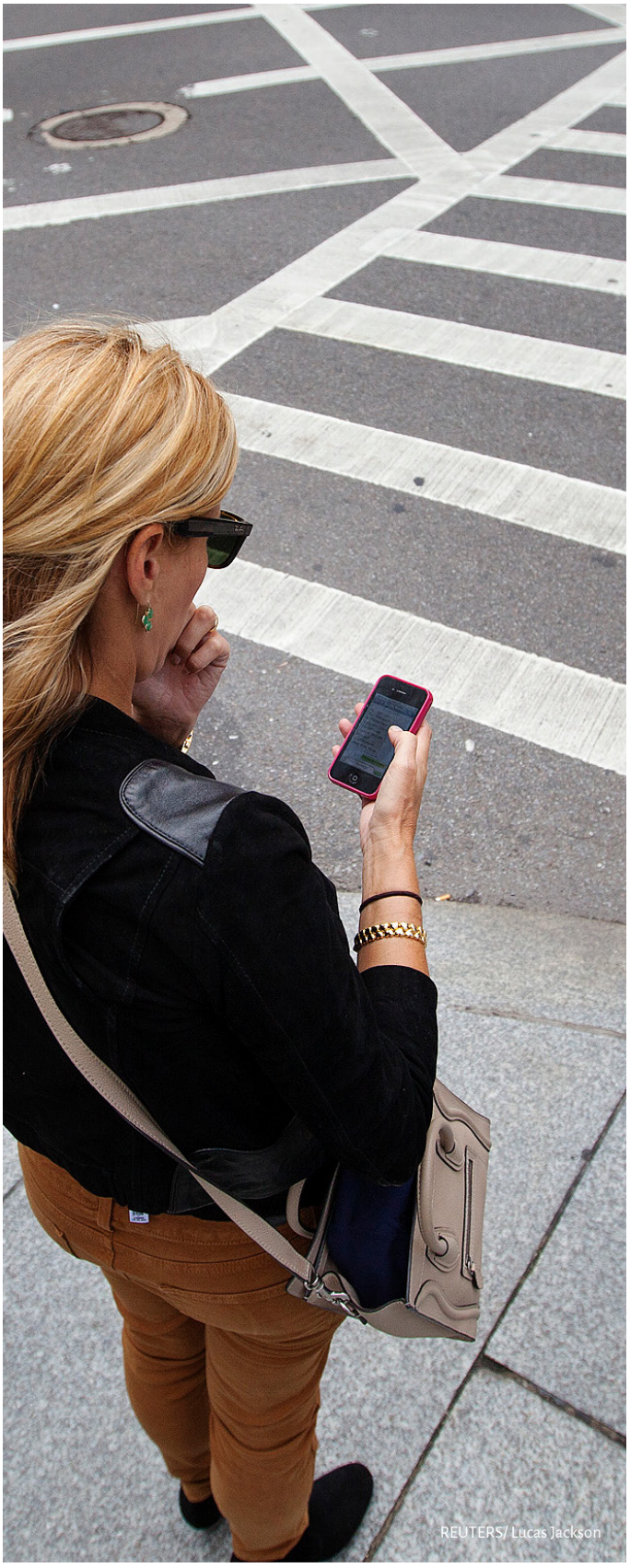
Although non-binding, the UNHCR Sexual and Gender-Based Violence Against Refugees, Returnees and Internally Displaced Persons: Guidelines For Prevention And Response[142] emphasizes that sexual exploitation is one of the main purposes of trafficking, and that trafficking for sexual exploitation can be committed by persons "in positions of power… including humanitarian aid workers, soldiers/officials at checkpoints, teachers, smugglers, and trafficking networks."[143] However, it does not make any specific reference to online aspects of sex trafficking.

The Sustainable Development Goals include targets on addressing trafficking for the purpose of sexual exploitation. Goal 5.2 calls on governments to "eliminate all forms of violence against all women and girls…, including trafficking and sexual and other types of exploitation".[144] Goal 16.2 calls for an end to "abuse, exploitation, trafficking and all forms of violence against and torture of children".[145] As with the other international standards, these goals do not refer to the use of the internet and digital technologies in the trafficking of women and children.

India has ratified the South Asian Association for Regional Cooperation (SAARC) Convention on Preventing and Combating Trafficking in Women and Children for Prostitution (SAARC Convention) which focuses primarily on the trafficking of women and children for the purpose of prostitution.[146] The Convention also places obligations on governments to ensure "trafficking in any form" is an offense under criminal law and is punishable by "appropriate penalties which take into account its grave nature". However, the instrument does not specifically refer to online aspects of trafficking.

In Africa, the Maputo Protocol, which Kenya and Nigeria have ratified, addresses trafficking and calls on States Parties to prohibit the recruitment (or buying) of persons for the purposes of exploitation.[147] The CRC Optional Protocol also has provisions calling on States Parties to "prevent and condemn trafficking in women, prosecute the perpetrators

136 UN Office on Drugs and Crime. (UNODC). Global Report on Trafficking in Persons, 2020. https://www.unodc.org/unodc/data-and-analysis/glotip.html
137 Article 6 of CEDAW
138 CEDAW Committee General Recommendation 38 (2020) on trafficking in women and girls in the context of global migration. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW/C/GC/38&Lang=en
139 CEDAW Committee General Recommendation 38 (2020). Paragraph 73
140 CEDAW General Recommendation 38 (2020). Paragraph 74
141 CRC Committee General Comment 25 (2021) on the rights of children in the digital environment
142 UN High Commissioner for Refugees (UNHCR). (2003). Sexual and Gender-Based Violence against Refugees, Returnees and Internally Displaced Persons. Guidelines for Prevention and Response. https://www.unhcr.org/protection/women/3f696bcc4/sexual-gender-based-violence-against-refugees-returnees-internally-displaced.html
143 Page 16 of the UNHCR Guidelines
144 https://unstats.un.org/sdgs/metadata/
145 https://unstats.un.org/sdgs/metadata/
146 Article I of the SAARC Convention
147 Article 4 of the Maputo Protocol. https://www.un.org/en/africa/osaa/pdf/au/protocol_rights_women_africa_2003.pdf


REUTERS/ Lucas Jackson

of such trafficking and protect those women most at risk"[148] and addresses the responsibility of States Parties to protect the rights of women and to establish measures to eradicate gender-based violence.[149] The CRC Optional Protocol applies to adult women and girls. Although the CRC Optional Protocol could be interpreted to include online trafficking, it is not specifically mentioned.

European Law and Standards

The EU Anti-Trafficking Directive on preventing and combating trafficking in human beings and protecting its victims[150] provides for EU states to take measures to ensure prosecution of offenders as well as effective protection of all trafficked persons. It states: "Exploitation shall include, as a minimum, the exploitation of the prostitution of others and other forms of sexual exploitation, forced labor or services, including, slavery or servitude, or the exploitation of criminal activities, or the removal of organs."[151]

In addition, the Victims of Crime Directive[152] calls on Member States to ensure victims of crimes such as sex trafficking receive appropriate information, support and protection, and are able to participate in criminal proceedings.[153] Member States are required to cooperate to improve victims' access to their rights afforded in the Directive.[154]

The EU Directives do not explicitly refer to online or digital technology aspects of sex trafficking.

Laws in Four Focus Countries

India, Nigeria, the UK, and the US have ratified the Palermo Protocol, and, with the exception of the US, the other four focus countries have ratified CEDAW. All focus countries have anti-trafficking laws which prohibit and penalize sex trafficking.

India

In India, the Penal Code makes it a criminal offense to recruit, transport, harbor, transfer or receive a person for the purpose of exploitation by using threats, any form of coercion, abduction, fraud or deception, abuse of power, or inducement of benefits to obtain the person's consent.[155] Further, it is an offense to sexually exploit a person in any manner if there is reason to believe the victim has been trafficked.[156] It is also an offense to sell and buy a child with the intent to use them for any "unlawful or immoral purpose".[157]

148 Article 4(2)(g) of the Maputo Protocol
149 The Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol). https://www.un.org/en/africa/osaa/pdf/au/protocol_rights_women_africa_2003.pdf
150 The EU Anti-trafficking Directive 2011/36/EU available at https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201136eu_en
151 Article 22 (3) of the EU Anti-Trafficking Directive
152 Directive 2012/29/EU of the European Parliament and the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA available at https://ec.europa.eu/anti-trafficking/sites/default/files/directive_2012_29_eu_1.pdf
153 Article 1(3) of the Victims of Crime Directive
154 Article 26 of the Victims of Crime Directive
155 Section 370 of the Indian Penal Code 1860
156 Section 370A of the Indian Penal Code 1860
157 Sections 372 and 373 of the Indian Penal Code 1860

Nigeria

Nigeria's federal trafficking statute, the Trafficking in Persons (Prohibition) Enforcement and Administration Act,[158] criminalizes all forms of human trafficking and expressly outlaws the procurement, recruitment, importation, and exportation of persons for the purposes of prostitution. The Act contains provisions specifically relating to the procurement or recruitment of those aged under 18. In addition, the Child Rights Act provides for the protection of the rights of children and criminalizes the buying, selling, and use of children for the purposes of begging, prostitution, and producing CSAM.[159]

UK

The UK's Modern Slavery Act[160] stipulates in Section 3 that sexual exploitation involves the commission of an offense under Section 1(1)(a) of the Protection of Children's Act (indecent photographs of children)[161] or under Part 1 of the Sexual Offences Act.[162] Sexual exploitation in the Act is defined broadly and can be interpreted to refer to exploitation that takes place both online and in person. However, there are recommendations that the UK should amend the law to more clearly reflect that a child is not able to consent to any element of their trafficking.[163] This is especially important in the online world, where adolescent girls are particularly vulnerable to being groomed online and trafficked.

US

In the US, there are federal statutes that provide against sex trafficking. The Trafficking Victims Protection Act criminalizes trafficking for sexual exploitation, which it defines as the recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a person for the purposes of a commercial sex act, in which the commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such an act has not attained 18 years.[164] Significantly, the law further defines any act of commercial sex with a person under the age of 18 years as "a severe form of trafficking".[165]

There are also federal statutes that focus on trafficking of children for sexual exploitation. These include the sex trafficking of children by force, fraud, or coercion statute.[166] This federal statute makes it illegal to knowingly recruit, entice, harbor, transport, provide, obtain, or maintain a minor. The statute also makes it a criminal offense to participate in a business venture that causes minors to engage in commercial sex acts. The transportation statute,[167] coercion and enticement statute,[168] the transportation of minors statute,[169] and the use of interstate facilities to transmit information about a minor statute[170] all criminalize the sexual exploitation and abuse of children in any form. The use of technology in trafficking is only mentioned in the coercion and enticement statute which prohibits the promotion or facilitation of sex trafficking through the use of mail, technology, or by way of telephone.

Of all the focus countries, the US is making the most efforts to legislate around the online and digital technological aspects of sex trafficking. In response to the growing crisis of online sex trafficking across the country, the US passed the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA-SESTA).[171] FOSTA-SESTA amends the "safe harbor rule" clause under Section 230 of the Communications Decency Act (CDA)[172] to clarify that the clause does not prohibit the enforcement of federal and state criminal and civil laws that penalize the providers and users of interactive computer services which knowingly facilitate, assist or support sexual exploitation for sex trafficking, prostitution, and for other purposes. Victims can now sue entities that helped advertise and traffic them online.

Conclusion

Although there is clarity on what constitutes sex trafficking, the online and digital technology aspects of this crime are neither specifically addressed in international law and instruments nor in regional and national laws (except to some extent in the US). Although in theory anti-trafficking laws could be applied to offenses that take place online or through the use of the internet, the extent to which perpetrators will be brought to justice in these situations requires further study.

158 Trafficking in Persons (Prohibition) Enforcement and Administration Act 2015
159 Please note that the Child Rights Act applies only to 24 out of 36 states in Nigeria. In the states where the Child Rights Act is not applicable, the CRC applies.
160 Modern Slavery Act, 2015 (U.K). https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted
161 Protection of Children Act 1978 available at Protection of Children Act 1978 https://www.legislation.gov.uk
162 Sexual Offences Act, 2003 (UK). https://www.legislation.gov.uk/ukpga/2003/42/contents
163 Independent Review of the Modern Slavery Act 2015: Final Report. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803406/Independent_review_of_the_Modern_Slavery_Act_-_final_report.pdf at page 17
164 Section 102 of the Victims of Trafficking and Violence Protection Act, 2000 (US). https://www.govinfo.gov/content/pkg/PLAW-106publ386/pdf/PLAW-106publ386.pdf
165 Section 103 (8) of the Victims of Trafficking and Violence Protection Act, 2000 (US)
166 18 U.S.C § 1591
167 18 U.S.C. § 2421
168 18 U.S.C. § 2422
169 18 U.S.C. § 2423
170 18 U.S.C. § 2425
171 Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (US). https://www.govinfo.gov/content/pkg/PLAW-115publ164/pdf/PLAW-115publ164.pdf
172 Section 230 of the Communications Act of 1934 (US)

Ruby - UK
Survivor Story

This interview was shared with Equality Now through #myimagemychoice, a survivor-led coalition asking for trauma-informed global laws and policy on intimate image abuse.

I'm a 28-years-old teacher and I first became aware of explicit images being shared because my friend's sister was a victim. She was alerted by a girl she knew saying, "I'm really sorry, my boyfriend's seen this image board". She was devastated and really confused about how they'd emerged on the Internet because the photos had never been sent anywhere.

She kept it quiet because my hometown is very small, people talk. So she just reported it to the police and didn't want to draw much attention. Six months later I got a message from a friend saying, "I'm on this explicit image board website and your picture, unfortunately, is next to mine."

The photos were of me aged 17, topless sunbathing on holiday. They'd been on Facebook ten years ago, only for a month before I'd taken them down. There were around 900 photos in the album and these were buried in the middle. Only friends could view them so it's definitely someone familiar with my Facebook profile. I thought who do I know that would want to attack me in that way?

It felt like a race against time because online media can be shared and spread so quickly. I just wanted someone to take the images down so it didn't snowball. I went to the police station and the desk officer took a report. By the end of that day, the police had received over 30 reports of women who've been affected. There was an influx because of girls alerting each other. In total, there are around 100, and many of the images were very explicit.

I think there is a network of perpetrators and definitely local because they knew so much detail - family connections, where people went to school, first names and sometimes surnames. The more threatening ones were when they knew where people worked. That was scary because it adds another level of threat.

The website was on a foreign server and seems set up to facilitate these kinds of crimes. The link we were sent was a thread for our local area, but there were so many on there, every country, every continent. We temporarily got the thread blocked. When I say we, I mean a group of victims that banded together, not the police. We reported it to the site owner and temporarily got a link suspended, but then it popped up elsewhere.

We set up a WhatsApp group to share communications on what's happening and support each other. It was really useful because it showed a lot of inadequacies in the investigations. Just from us victims speaking, we could identify connections between the girls and people in the screenshots. We were never asked the names and the local perpetrator element didn't seem to be pursued by the police.

This was a gendered crime and there was an element of victim blaming. After I reported, I got a call from an officer saying things like, "There's not a lot we can do. The website is hosted on a foreign domain. We can't shut it down UK side because we have no jurisdiction." I don't think he took it seriously and inferred it's kind of your fault for putting the photos up there. That's not the response you should get, this is a crime regardless of where the photos were.

We complained and got the case transferred to a female officer. She was better but things went quiet and a month later we got an email saying the case had been closed and passed to the regional Organized Crime Unit and Cybercrime Unit. No reference or contact details.

We weren't happy so we penned a letter to the Chief Constable outlining everything that had gone wrong. We wanted to change things so future victims don't go through the same terrible experience. We met the Superintendent and it came to light that every report had been categorized differently. If it was recorded as hacking, it went to the Cyber Crime Unit. If the girls said they'd sent pictures to an ex-boyfriend, this was logged but not classified as a crime, even though they were intimate images shared without consent. None of cases were linked together, despite the majority of reports being made on the same day about the same website.

We've been let down by the justice system and it's left us feeling quite helpless and hopeless that there's been no prosecution. Nothing has been done to stop that happening to someone else. That this crime is so difficult to prosecute is really frustrating and angers me. People can get away with it far too easily and perpetrators are well aware nothing is going to happen to them.

Image-Based Sexual Abuse

Image-based sexual abuse is the non-consensual distribution of sexually explicit images or videos of an individual.[173] It includes images taken consensually but accessed and then shared without consent, as well as voyeurism,[174] sexual coercion and extortion, recordings of sexual assaults,[175] and image manipulation such as deepfakes. Deepfake sexual abuse uses people's faces and voices "to generate digital doppelgängers".[176] Faces are superimposed on bodies, and it is very difficult to tell the difference between the fake and real images, so the harm to victims is just as significant. Image-based sexual abuse has become more prevalent with the advent of social media and easily accessible and useable devices and software.[177]

International Law and Standards

Taking and sharing intimate images without consent is an invasion of one's right to privacy. On that basis, international instruments such as Article 12 of the Universal Declaration of Human Rights[178] and Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[179] could apply, as they protect from arbitrary or unlawful interference with people's privacy, reputation, and dignity.

Image-based sexual abuse involving children is covered by some Council of Europe conventions on child abuse. For example, the Lanzarote Convention calls for States Parties to criminalize all forms of sexual offenses against children.

European Law and Standards

In the case of adults, many European countries could apply privacy laws.[180] Additionally, the right to protection of individual privacy is protected under the European Convention on Human Rights.[181] Specifically, Article 8 of the European Convention on Human Rights provides that "everyone has the right to respect for his private and family life, his home and his correspondence" with limitations only in accordance with the law and as is necessary in a democratic society for the protection of specific objectives including the prevention of crime, the protection of health and morals and the protection of the rights and freedoms of others. Article 8 can be interpreted to protect people from having their sexual images shared online without their consent.

In addition, the provisions of the EU General Data Protection Regulations (GDPR) providing for protection of individual privacy may also apply to image-based sexual abuse.[182] However, privacy provisions alone do not provide for

Unsplash/Laura Chouette

173 Glossary on platform law and policy consolidated after IGF. https://www.intgovforum.org/multilingual/content/glossary-on-platform-law-and-policy-terms
174 Hirschfeld, M. (1938). Sexual anomalies and perversions: Physical and psychological development, diagnosis and treatment. London: Encyclopaedic Press
175 Op. cit. Note 7
176 https://www.dacbeachcroft.com/en/gb/articles/2020/september/the-legal-implications-and-challenges-of-deepfakes/
177 Magaldi, Jessica A. and Sales, Jonathan S. and Paul, John. (2020). Revenge Porn: The Name Doesn't Do Nonconsensual Pornography Justice and the Remedies Don't Offer the Victims Enough Justice. Oregon Law Review, Vol. 98, No. 1. https://ssrn.com/abstract=3527819
178 https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
179 https://www.ohchr.org/documents/professionalinterest/ccpr.pdf
180 Rotenberg, Marc. Jacobs, David (2013). Updating the Law of Information Privacy: The New Framework of the European Union. Harvard Journal of Law and Public Policy. 36 (2). http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_Rotenberg_Jacobs.pdf
181 Article 8 of the European Convention on Human Rights. https://www.echr.coe.int/documents/convention_eng.pdf
182 EU General Data Protection Regulation 2016/679. https://gdpr-info.eu

adequate protection because image-based sexual abuse "is perpetrated for reasons of entitlement, power and control, and most victims are female", while privacy-related offenses "do not necessarily impact one gender more than the other, and they do not arise out of patterns of gender inequality".[183] There is a need for provisions that specifically address image-based sexual abuse. A more in-depth discussion on some of the provisions in the GDPR will be had in the privacy section below.

Laws in Five Focus Countries

Kenya

In Kenya, criminal defamation charges, which were made to hold offenders of image-based sexual abuse accountable, were challenged[184] on the grounds that prison sentences infringed on the right to freedom of expression, and the court agreed. Following this case, victims of image-based sexual abuse can still use the Penal Code[185] to hold offenders accountable for defaming them, but the courts will not sentence the offenders to any jail time.

Victims can bring civil law claims including the infringement of privacy and copyright and the intentional infliction of emotional distress. However, there are limitations. For instance, under Kenya's Copyright Act,[186] victims may only have recourse if they can establish authorship of the image or video in question. Invoking one's right to privacy under Kenya's Data Protection Act[187] may be a better remedy, even though this brings other challenges, as discussed below in the section dealing with digital rights.

UK

Prosecution of this offense may also come under the Communications Act, the Malicious Communications Act, and the Protection from Harassment Act. In England and Wales, the Criminal Justice and Courts Act creates a specific offense for someone to disclose private sexual photos and films.[188] The Act requires proof of several elements: that there was sharing of a private sexual photograph or film; without the consent of the person depicted in the photograph or film; and with the intention of causing distress to the person depicted.[189]

The Act has resulted in prosecutions, but there are gaps as some aspects of the offense are not criminalized. For example, the law does not criminalize threats to share sexual images or the production and sharing of technologically generated images depicting a known person (such as deepfakes).[190] In addition, the law does not take into account sharing where the motivation is other than causing distress, such as sharing with the intention of obtaining a profit or for entertainment. Lawyers have said access to justice for victims is still a challenge.[191] At the time of writing, the UK's Law Commission was undertaking a consultation process on non-consensual sharing of sexual, intimate material.[192]

US

In the US, 48 states have laws that criminalize image-based sexual abuse. For example, New Jersey state law prohibits the non-consensual recording of someone's intimate body parts and the non-consensual distribution or sharing of that recording.[193] California's Penal Code[194] makes it an offense to post explicit images of someone online without their consent.

However, some state laws are flawed or include unnecessarily burdensome requirements that create roadblocks for victims to be protected from image-based sexual abuse. For example, Arizona law[195] additionally requires an "intent to harm or harass", or for the offender and victim to be in a domestic relationship.

India

In India, cases of image-based sexual abuse may be prosecuted under the Information Technology Act,[196] the Penal Code,[197] or the Indecent Representation of Women (Prohibition) Act,[198] Image-based sexual abuse was defined in a judgment of a first instance criminal court in the Indian state of West Bengal (in what is considered to be the first prosecution of this offense in India) as "sexually explicit

183 The Sydney Morning Herald. (September 2015) 'Revenge porn' needs more than a slap on the wrists. https://www.smh.com.au/opinion/revenge-porn-laws-need-to-be-more-robust-and-comprehensive-20150914-gjm0t6.html#ixzz3m1KdlKJC
184 *Jacqueline Okuta & another v. Attorney General & 2 others* [2017] eKLR
185 Section 194 of the Penal Code, 2018 (Kenya)
186 Copyright Act, 2001 (Kenya). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/CopyrightAct_No12of2001.pdf
187 http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
188 Section 33 of the Criminal Justice Act 2015. https://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted
189 Section 33 of the Criminal Justice Act 2015
190 https://www.gov.uk/government/news/law-around-non-consensual-taking-making-and-sharing-of-sexual-images-to-be-reviewed
191 https://www.leighday.co.uk/latest-updates/blog/2018-blogs/revenge-porn-and-the-law/
192 http://www.lawcom.gov.uk/project/taking-making-and-sharing-intimate-images-without-consent/
193 New Jersey statute section NJSA 2C:14-9
194 Section 647(j) (4) of the Penal Code (US)
195 Arizona Revised Statute §13-1425. https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/13/01425.htm
196 Section 66E (violation of privacy, publishing or transmitting obscene material in electronic form), section 67 (publishing or transmitting of material containing sexually explicit act) and section 67A (publishing electronic material containing sexually explicit act).
197 Section 292 (distribution and circulation of obscene material), section 354C (capturing or dissemination of pictures of a woman engaged in a private act without her consent), section 499 (act done by a person intending to harm or having reason to believe the same would harm an individual's reputation or character) and section 509 (act intended to insult the modesty of a woman). These provisions relate to voyeurism and the non-consensual sharing of consensually captured images. It should be noted that section 354C and section 509 have gendered application and presume a male offender and a female victim.
198 Section 4 of the IRWA prohibits the publishing of photographs which contain indecent representation(s) of women.


REUTERS/Adnan Abidi

images of a person posted online without that person's consent especially as a form of revenge or harassment".[199]

Nigeria

In Nigeria, the Criminal Code Act and the Cybercrimes (Prohibition, Prevention, etc.) Act provides for some aspects of image-based sexual abuse but not specifically online.[200] The Criminal Code Act prohibits knowingly sending or attempting to send by post an "indecent or obscene print".[201] The provision could perhaps be interpreted to apply to online image-based sexual abuse. Notwithstanding, the Cybercrimes (Prohibition, Prevention, etc.) Act prohibits knowingly distributing material which is "grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent… or he knows to be false for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent" through a computer system or network.[202] This section provides for the posting or sharing of image-based sexual abuse on the internet.

Conclusion

There are no legal instruments that address image-based sexual abuse at the international level. There are different efforts across the focus countries to address the harm but there are many gaps. One glaring gap is that deepfakes are not addressed in law. Deepfakes cause harm to victims. Offenders can also use the images to coerce or extort their victims.

Apart from prosecution of the crime, image-based sexual abuse can also be addressed through takedown notices, i.e. when victims request digital service providers and platforms to remove and stop further sharing of the images.[203] However, this has not been helpful in all situations as service providers and platforms, which are designated as conduits of third-party content, are exempt from liability except in certain circumstances. This may be complicated by the fact different platforms have different standards. The specific challenges are discussed in more detail in the sections below.

199 *State of West Bengal v. Animesh Boxi*, C.R.M. No. 11806 of 2017, GR/1587/2017 at page 105. https://globalfreedomofexpression.columbia.edu/cases/state-of-west-bengal-v-boxi/
200 Manfield Solicitors. Revenge Porn and the Nigerian Law. https://www.manifieldsolicitors.com/2018/12/12/revenge-porn-and-the-nigerian-law/
201 Section 170 of the Criminal Code Act, 1990 (Nigeria)
202 Section 24 of the Cybercrimes Act of Nigeria 2015 (Nigeria)
203 InternetLab. (2018). How do countries fight the non-consensual dissemination of intimate images? https://www.internetlab.org.br/wp-content/uploads/2018/11/Fightijng_the_Dissemination_of_Non.pdf

Dr. Debarati Halder
Expert Interview

Managing Director,
Centre for Cyber Victims Counselling - India

I have observed an explosion in different types of online victimizations targeting women and children, and it is becoming very common. I have dealt with cases that fit all patterns of online sexual abuse, including grooming, image-based sexual abuse, and online sexual coercion and extortion.

Perpetrators are found across age ranges. For example, there are instances where children are abused by their own peers in WhatsApp groups and via social media platforms like Instagram. Of particular concern is that victims and perpetrators of image-based sexual abuse are particularly prevalent amongst teenagers.

The Information Technology Act, 2000, was amended in 2008 with one provision addressing [CSAM]. Other than this, we have a colonial era Penal Code as the central law. This statute has some provisions that prevent obscene contents and circulation of such contents to children. But with the 2008 amendments to the Information Technology Act, and the introduction of new acts like the POCSO Act in 2012, several issues of online child sexual abuse are addressed.

However, the new amendments did not cover sexting, image-based sexual abuse, bullying, or trolling. These are covered using existing statutes in the Indian Penal Code, POCSO Act, IT Act etc. These types of offenses must be recognized and gaps in cyber law closed. The limited accountability of website platforms also needs to be addressed.

The long existing void has created space for perpetrators to exploit children online. This includes showing or grooming children for sexual exploitation purposes, using children for pornographic purposes, and sharing sexually explicit images with children.

Child-related victimization laws are improving but India lacks proactive mechanisms to trap offenders. Some cases are booked by police but few go to trial. In most cases, especially in rural areas, the police lack training in how to investigate cybercrimes, handle evidence, and deal with victims. Access to technology is also an obstacle.

Police without specialist training may not understand the nature of the crimes. Victim blaming, and caste and class discrimination are also problems. But when it comes to prosecution, there are strict guidelines that the police and courts are required to follow.

It is important that complainants preserve evidence of abuse. Unfortunately, it is common for incriminating content to be deleted. Some families feel reluctant to take matters to the police and courts. Problems include slow reporting, vanishing digital footprints, and the withdrawal of cases for fear of further trouble. Social stigma and victim blaming by families and communities are also challenges but I have seen several families defending their victimized children.

There is a gradual improvement in raising awareness but it is crucial that more is done to sensitize children, with parents, teachers and other key players. First and foremost, people need to be aware of different types of cybercrimes and related laws. Precautionary advice should be easily accessible, including being taught about cyber security, data breaches and the risk of spyware and hacking software. Devices handled by children are especially prone to security breaches because children often download games and songs that may contain spyware software that can access private images.

However, it is also important that parental digital surveillance does not impinge on a child's privacy and dignity. Parents, educators, and caregivers need to act like digital guides, not cyber-stalkers. Close surveillance should only apply if there are clear indications that the child may be at risk or is potentially a perpetrator.

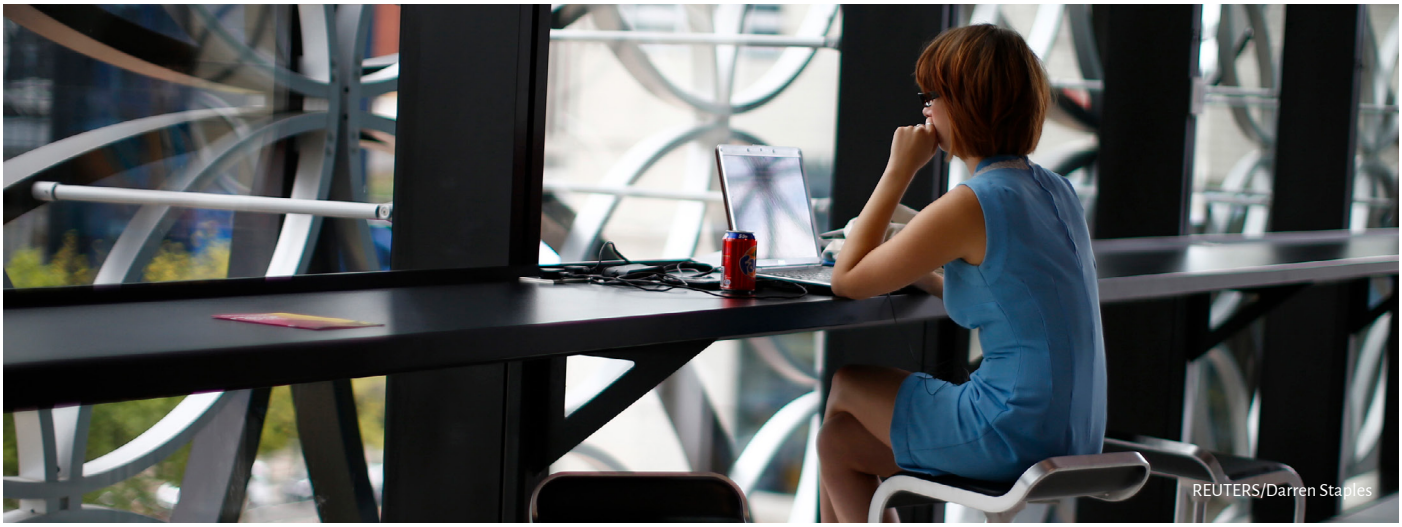
"I have observed an explosion in different types of online victimizations targeting women and children, and it is becoming very common. I have dealt with cases that fit all patterns of online sexual abuse, including grooming, image-based sexual abuse, and [online sexual coercion and extortion]."

CHALLENGES IN OBTAINING LEGAL RECOURSE FOR OSEA

There are several challenges when people seek legal recourse and redress after experiencing sexual exploitation and abuse online. There is widespread impunity, exacerbated by gaps in the laws, and the anonymity the internet affords offenders. Challenges include:

- The global and multi-jurisdictional nature of OSEA, where offenders, victims and technology platforms are often located in different countries, presents legal challenges concerning jurisdiction, the prosecution of offenders, and remedies for victims.
- How to balance between the fundamental values of an open internet (including privacy and freedom of expression rights) and the protection and safety of users.
- The regulation of digital service providers and platforms, and the lack of consistency across jurisdictions regarding their responsibility and liability for sexual harms on their platforms, balancing between the need for legal accountability, and digital service providers and platforms' innovation and voluntary practices.

Below we will examine the nature of each challenge.


REUTERS/Darren Staples

Establishing Territorial and Extraterritorial Jurisdiction in OSEA Cases

Jurisdiction refers to the authority of a territory to exercise power and for a court within a territory to adjudicate over a legal matter or case.[204] Online criminal activities present challenges because they are rarely confined to one country or territory where one legal system applies. The offending act can take place in a different country from where the harm is experienced, and the digital service provider or platform may be based in yet another country. In complex cases, there may be multiple perpetrators, multiple victims, and multiple platforms, all based in different countries making investigating and prosecuting cybercrime particularly challenging. It is difficult to hold perpetrators accountable due to issues related to which country has authority over the harm suffered, which country's laws are applicable, and which mechanisms can be used to prosecute them.

When looking at production, offenders generally do not care where children are from, especially when the victims are younger. Sometimes language is a bit of a barrier, but sites have different areas and there is cross communication.

International Frameworks for Establishing Jurisdiction for OSEA Crimes

The most relevant international agreements providing for the operation of territorial and extraterritorial jurisdiction to prosecute online sexual offenses are the Budapest Convention, the Lanzarote Convention, and the CRC Optional Protocol. Each Convention includes guidance on establishing jurisdiction, including extraterritorial jurisdiction for purposes of prosecution. These Conventions do not address all forms of OSEA but deal mainly with online sexual crimes against children, including CSAM, grooming, and solicitation of children for sexual exploitation and abuse.

Article 22(1) of the Budapest Convention provides that each State Party "shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offense established in accordance with Article 2 through 11 of this Convention" when the offense is committed in its territory; or by one of its nationals if it is a criminal offense where it was committed; or by one of its nationals if the offense is committed outside its territory but is a criminal offense in its territory. Article 22(2) limits the operation of this provision by stating that a State Party "may reserve the right not to apply

204 www.law.cornell.edu.wex

Establishing Extraterritorial Jurisdiction

Example:

- **Offense is live-streaming of sexual abuse of a minor.**
- **Victim is a citizen of Country A in Country A.**
- **Perpetrator is a citizen of Country B in Country B.**
- **Online platform is domiciled in Country C.**

STEP 1

Determine the victim's nationality and location.

Determine the perpetrator's nationality and location.

STEP 2

Determine where the offense occurred.

Online

Determine where the online platform is domiciled.

STEP 3

Determine what offense was committed and the victim's age.

STEP 4

Determine if the offense is recognized as a crime in each location.

Country of victim | **Country of perpetrator** | **Country where offense occurred**

STEP 5 CONSIDERATIONS

Suppose the offense is a crime in Country A

Can Country A prosecute the perpetrator, a citizen of Country B?

Yes, if there is:

A binding treaty

If Country A and Country B are parties to a treaty that makes live-streaming of sexual abuse a legal offense, the two countries must assist each other in prosecuting the crime. They can agree on whether to prosecute the perpetrator in Country B or extradite the perpetrator to Country A.

A mutual assistance agreement

If Country A and Country B have a mutual assistance agreement, the two countries can manage the perpetrator's prosecution under the agreement.

An extradition agreement

Country A can request Country B to extradite the perpetrator to face prosecution in Country A.

A formal agreement

The two countries can reach a formal agreement on the perpetrator's prosecution.

Suppose the offense is a crime in Country B

Can Country B prosecute the perpetrator?

Yes

Country B law applies

The perpetrator is a citizen of Country B and committed the crime in Country B.

EVIDENCE GATHERING

How can Country A or Country B obtain evidence of the crime from Country C's online platform?

Through Country C's law

The online platform is bound by Country C's law.

Through a binding treaty or mutual assistance agreement

If applicable, a binding treaty or mutual assistance agreement between Country C and either Country A or Country B.

Steve Grocki
Expert Interview - Part 2

Chief of the Criminal Division's Child Exploitation & Obscenity Section, US Department of Justice

When you are looking at production, offenders generally don't care what country children are from, especially when the victims are younger. They will target children wherever it is easy to do so, regardless of nationality or language. Sometimes language is a bit of a barrier but sites have areas dedicated to specific common languages and it is easy to use online translation services to understand communication in another language.

TOR gives great insight into how these global networks work. Hidden services (websites) on TOR operate as a global community and there are offenders all round the world represented, although many of the larger players are in Europe and America. This cross border activity increases the complexity enormously and makes it very difficult to investigate offenders when they are utilising platforms outside of the US, even if they are based in America.

As offenders are located globally, we are more reliant than ever on foreign countries to respond. It makes investigations much more challenging because we have to employ international mechanisms which can cause huge delays in getting access to evidence or offenders. It's even harder to investigate and punish offenders when they are based in places like Africa, Asia and Latin America where law enforcement capacity and subject matter expertise may be challenged.

In many parts of the world there are fundamental deficits in resources which mean investigators and survivors don't have access to the same legal remedies, victim support services, and online forensics that are available in the U.S. Through the U.S. State Department, we are sharing lessons learned in developing and implementing laws in America. For example, via the WePROTECT Global Alliance Model National Response, we have been training people working in African countries, where mobile phone infrastructure is improving, more kids are getting access to devices, and there is a corresponding increase in CSAM.

We are seeing many of the same things we come across in Western countries but its emerging at a much more accelerated speed in Africa. In Western countries, when people first obtained smartphones, tablets and laptops, the same platforms weren't available and cloud storage was much smaller. Now the online world is highly developed and you are entering a realm that is far more dangerous. There are a vast number of people coming online that aren't digital natives, don't know the potential risks, and as result, may have difficulty keeping children safe.

or to apply only in specific cases or conditions the jurisdiction rules..." under Article 22(1).

Article 4 of the CRC Optional Protocol includes additional criteria when the offense has been committed on board a ship or aircraft registered in the State Party; where the alleged perpetrator is a resident of its territory; or where the victim is a national of its territory. The CRC Optional Protocol also provides that if a State Party does not extradite one of its nationals relating to an offense in another territory/country, the Member State would have jurisdiction to prosecute the national for that offense in its own courts.[205]

The Lanzarote Convention takes a similar approach and establishes various forms of sexual abuse as criminal offenses, contains preventative measures or policies to be implemented at the national level, and seeks to protect the rights of child victims by outlining national measures to promote and protect victims' rights. Under Article 25(1) of the Lanzarote Convention "each Party shall take the necessary legislative or other measures to establish jurisdiction..." when offenses under the Lanzarote Convention are committed either in its territory; or on board a ship flying the flag of that Party; or on board an aircraft registered under the laws of that Party; or by one of its nationals; or by a person who has their habitual residence in its territory; or where the offense is committed against one of its nationals or against a person who has his or her habitual residence in its territory. Article 25(3) limits the operation of this jurisdictional provision by stating that a State Party "may... declare that it reserves the right not to apply or to apply only in specific cases or conditions the jurisdiction rules" under Article 25(1).

The three instruments also provide rules for establishing jurisdiction where more than one country claims jurisdiction. Where multiple countries are involved, Article 22(5) of the Budapest Convention provides that "the Parties involved shall,

205 Article 5 (5) of the CRC Optional Protocol. 2002. https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx

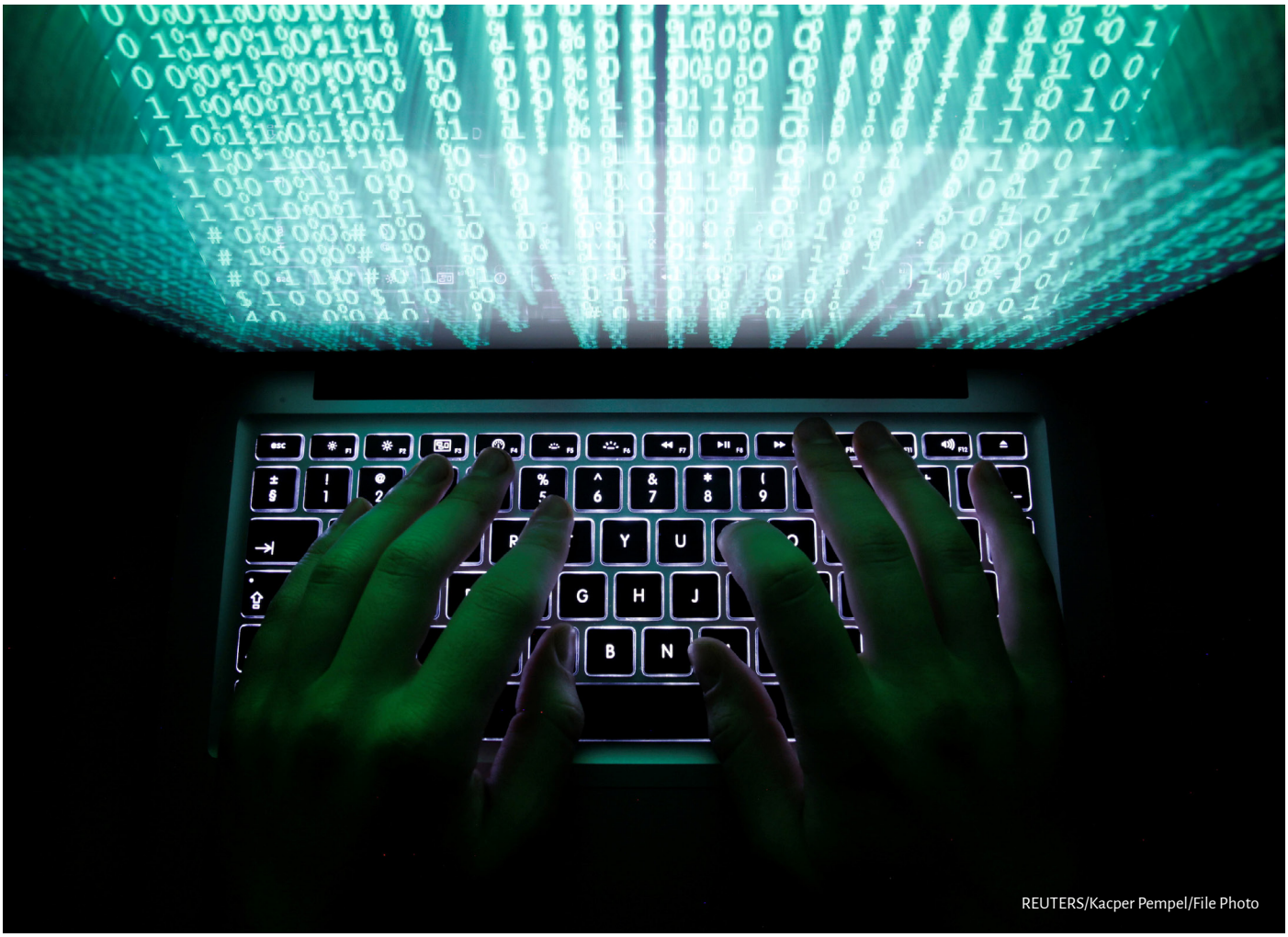
where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution". The Lanzarote Convention has similar provisions.[206]

The Budapest Convention also calls for States Parties to cooperate in the collection and gathering of evidence. Article 23 mandates them to "cooperate with each other... and through the application of relevant international instruments on international co-operation in criminal matters, [make] arrangements on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence".

The need for cooperation is also underscored in Article 6 of the CRC Optional Protocol which requires States Parties to cooperate and provide one another with "the greatest measure of assistance in connection with investigations or criminal or extradition proceedings". Article 7 calls on States Parties to "execute requests from another State Party for seizure or confiscation of goods, for example instrumentalities used in the commission or facilitation of offenses or proceeds".[207]

European Frameworks for Establishing Jurisdiction for OSEA Crimes

In Europe, the EU Combating Sexual Abuse of Children Directive has provisions for establishing jurisdiction for sexual crimes against children. The Directive provides for broader jurisdiction related to crimes committed by nationals of other EU Member States. In particular it requires Member States to establish jurisdiction for the offenses in the Directive, within the specific country and over its residents.[208] A State can also establish jurisdiction where the offense is committed using "information and communication technology accessed from their territory, whether or not it is based on their territory".[209] The Directive also requires a Member State to take necessary measures to ensure "its jurisdiction is not subordinated to the condition that the acts are a criminal offence at the place where they were performed" and "that the prosecution can only be initiated following a report made by the victim in the place where the offence was committed, or a denunciation from the State of the place where the offence was committed".[210]



REUTERS/Kacper Pempel/File Photo

206 Article 25 (6) of the Lanzarote Convention

207 Further examples of cooperation provisions include: Article 25(8) of the Lanzarote Convention which states that "When more than one Party claims jurisdiction over an alleged offense established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution"; and Article 38 of Lanzarote Convention sets out further general principles and measures for international cooperation.

208 Article 17(1) & (2) of the EU Combating Sexual Abuse of Children Directive

209 Article 17 (3) of the EU Combating Sexual Abuse of Children Directive

210 Article 17 (4) & (5) of the EU Combating Sexual Abuse of Children Directive

Sarah Kuponiyi
Expert Interview

ImSafer Instructor,
Center for Clinical Care and Clinical Research - Nigeria

I've come across lots of girls who have experienced online harassment, abuse, or exploitation, particularly via Facebook. A girl starts chatting to someone online, they communicate for a while, have private chats, and she thinks they're in a relationship. Guys say sweet words, especially to girls who are vulnerable and in need of a job or money. Sometimes they make plans to meet in person and she ends up being raped.

Another very common problem is intimate photographs being leaked, or used to blackmail someone. Nigeria has a law against nude pictures being posted without consent but in most cases the victims are too scared to report when it happens.

There are also cases of girls being trafficked after they have been tricked online. Frequently they are offered jobs, sometimes outside of the country, and then are coerced into prostitution.

Online abuse is a problem everywhere but the situation is worse in urban areas where there is more access to the internet. Wherever it happens, the culture of victim blaming is prevalent and responsibility is generally placed on the woman or girl. People say, "Why did you do that? What were you thinking? What is so special about your body that you are trying to report something?"

Experiences like this can have a big impact on a victim's mental health and often it affects their academic performance. It damages how they view the opposite sex and they feel like they can't trust anyone anymore.

A girl can't go to the police because most officers won't listen to her. They say it should be a parent who reports it. The police also think that sexual harassment is normal. I have been to a police station to report a sexual assault case and the officer said, "Why don't you just let the matter die down, it was only touching."

Another challenge is that police will ask for a filing fee and this frustrates whoever goes to report. As a social worker you have to use your own money to pay when you are reporting a crime on behalf of a victim. Most people get discouraged with the justice system and rather than go through the stress of reporting, they would rather keep things to themselves.

The police don't understand the nature of online abuse and I don't think it is something they are thinking about. There also isn't much awareness within the government or schools. NGOs are doing a lot to teach girls about to how to protect themselves from sexual abuse, and are providing awareness training for police. But unfortunately, I am not seeing much change in the wider society and the fact that boys and men know they aren't going to get caught encourages them.

We need more awareness and better systems in place to punish perpetrators. When someone comes to report a case of online sexual abuse, they shouldn't be invalidated by the police or made to feel like it was nothing. They should feel confident that it will be taken seriously and something will be done by the authorities.

Online abuse is a problem everywhere but the situation is worse in urban areas where there is more access to the internet. Wherever it happens, the culture of victim blaming is prevalent and responsibility is generally placed on the woman or girl.

Mutual Assistance Laws and Agreements

When a government establishes extraterritorial jurisdiction over a person(s) who has committed an offense across multiple jurisdictions, all governments involved need to cooperate to ensure appropriate information and evidence is gathered and exchanged for prosecution purposes, and to allow extradition of the alleged offender(s) for prosecution. Bilateral and multilateral mutual legal assistance and extradition regimes facilitate these processes.

Mutual assistance legislation outlines the procedures that a country can use to request assistance from other countries to prosecute crimes. Usually, mutual assistance legislation provides the framework for a country to obtain sufficient information or evidence to prosecute or to undertake extradition procedures. Such arrangements exist based on provisions in national legislation, bilateral agreements, or multilateral conventions. A key example of a mutual assistance regime is the Convention on Mutual Legal Assistance in Criminal Matters[211] which provides the core basis for requests for mutual assistance between EU Member States. In the absence of an express requirement of mutual assistance, countries rely on goodwill or courtesy.

International Framework on Mutual Assistance Laws and Agreements

There is no formal global treaty that provides a framework for mutual assistance between governments on OSEA offenses. The UN Human Rights Council's open-ended intergovernmental working group's third draft of the legally binding instrument to regulate, in international human rights law, the activities of transnational corporations and other business enterprises (the Business and Human Rights Treaty) once in effect, will provide for mutual legal assistance and international judicial cooperation which will include initiating and carrying out investigations, prosecutions, and judicial and other criminal, civil, or administrative proceedings.

Presently, there are informal mechanisms for cooperation including the Global Prosecutors E-Crime Network and the voluntary sharing of information between police forces.

European Framework on Mutual Assistance Laws and Agreements

The Convention on Mutual Legal Assistance in Criminal Matters provides the framework for requests for mutual assistance between EU Member States. The European Cybercrime Centre can also facilitate coordination and execution of international mutual legal assistance requests. EU Member States also have bilateral agreements on extradition and mutual legal assistance with other countries, like the US, Japan, and Norway.

Mutual Assistance Laws and Agreements - Application in the Five Focus Countries

The focus countries have fairly developed laws that deal with mutual assistance in criminal matters.

Kenya

In Kenya, the Mutual Legal Assistance Act[212] sets out the procedures allowing the Attorney General to request legal assistance from another country. In Section 40 of the Act, Kenya may also provide assistance to a requesting country even in the absence of dual criminality and reciprocity. In addition, the Computer Misuse and Cybercrimes Act provides that the Attorney General and Department of Justice may request assistance from another country in any investigation related to a crime under the Act.

Nigeria

Nigeria's Mutual Assistance in Criminal Matters Act[213] governs the operation of reciprocal assistance between Nigeria and other countries, but it only operates when there is a bilateral mutual assistance agreement.

India

In India, the Code of Criminal Procedure[214] envisages reciprocal arrangements with other countries. In addition, India has entered into mutual assistance treaties with at least 39 countries. India's Ad Hoc Committee Report[215] recommends that the Ministry of Electronics and Information Technology seek to establish relationships with priority countries with which India has a mutual assistance treaty to fast-track requests to take down unlawful content. It also recommends that India should engage with the Virtual Global TaskForce, a group of law enforcement agencies from twelve countries plus Interpol, working to stop CSAM.

US

In the US, the Clarifying Lawful Overseas Use of Data (CLOUD Act)[216] provides a framework which allows foreign governments to issue orders requesting the production of information directly to US internet service providers. The US also relies on other cooperative mechanisms to prosecute online child sex offenses. For example, the US Immigration and Customs Enforcement Agency cooperates with foreign governments and can make arrests under the travelling child sex offender provisions of the 2003 Protect Act.[217]

The US also engages with an INTERPOL working group (working with internet service providers to block access

211 European Convention on Mutual Assistance in Criminal Matters. https://rm.coe.int/16800656ce
212 Mutual Legal Assistance Act 2011 (Kenya). http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2036%20of%202011
213 Mutual Assistance in Criminal Matters Act 2019 (Nigeria)
214 Code of Criminal Procedure 1973 (India)
215 Report on the Ad Hoc Committee Report, 2002 (India). https://niti.gov.in/writereaddata/files/Report%20of%20The%20AD-HOC%20Committee.pdf
216 Section 105 of the Cloud Act
217 Section 2252A(a)(3)(B) of Title 18 of the United States Code

to child abuse materials online), and the Virtual Global Taskforce (a multinational group of law enforcement agencies and private sector partners, identifying children at risk of online sexual offenses). The FBI Violent Crimes Against Children International Taskforce also has a role in preventing online sexual offenses against women and girls.

UK

In 2019, the UK entered into a data access agreement with the US.[218] The agreement allows UK police to directly approach US digital service providers and platforms to access data required to investigate and prosecute criminal offenses punishable by a maximum term of at least three years in the UK. The Agreement potentially increases the speed of data collection and efficiency of investigations and prosecutions. Like the US, the UK also engages with INTERPOL and is a member of the Virtual Global Taskforce.

Extradition

A key aspect of prosecuting online crimes is the location of the perpetrator(s) and, if outside the country where the offense will be prosecuted, how the perpetrator(s) can be brought to face criminal charges making extradition agreements crucial.

International Framework on Extradition

Ratified by all the focus countries, the UN Convention against Transnational Organized Crime[219] provides a notable international extradition framework. Article 16 of the Convention provides a basis for extradition requests where there is no other existing basis, relating to "serious crimes" committed transnationally. "Serious crimes" under the Convention are those punishable by at least four years of imprisonment.[220] Although the Convention primarily covers transnational organized crime offenses such as money laundering and engaging in corruption activities, it may extend to other serious crimes committed online not covered by the Convention for the purposes of an extradition request when these crimes are committed alongside the crimes covered by the Convention.[221]

Article 5 of the CRC Optional Protocol provides that the offenses under Article 3 (including "producing, distributing, disseminating, importing, exporting, offering, selling or possessing [CSAM]") must be included in extradition treaties of States Parties. Article 5 also provides that offenses are treated as if they had been committed in both the location where the offense occurred and in the State seeking to establish extraterritorial jurisdiction (that is, dual criminality is deemed to apply). Further, Article 5 provides that if the "requested State Party does not or will not extradite on the basis of the nationality of the offender, that State shall take suitable measures to submit the case to its competent authorities for the purpose of prosecution". In addition, Article 6 of the CRC Optional Protocol requires State Parties to assist one another relating to investigations or criminal or extradition proceedings.

European Framework on Extradition for OSEA Offenses

The European Arrest Warrant (EAW) can be used in the extradition of perpetrators of online sexual crimes. The warrant may be issued by either a Member State of the EU or a non-Member State with an agreement with the EU. When issuing an EAW, a Member State gives consideration to the seriousness of the offense committed, whether a custodial sentence would be imposed under its own national laws and the impact of the offense on victims. The operation of an EAW means that Member States can no longer refuse to surrender their own nationals unless they take over the execution of the prison sentence against the wanted person or unless the requesting Member State is not able to guarantee a fair trial.

The EU has also entered into bilateral extradition arrangements with other countries, like the US. Under those agreements, a perpetrator can be extradited if the offense is punishable in the EU Member States and the US by at least one year of imprisonment.

Extradition – The Experience Across the Five Focus Countries

UK

Extradition in the UK is governed by the Extradition Act[222] which provides for extradition arrangements between the UK and other countries. For example, the UK-US Extradition Treaty requires that an offense be punishable in both countries by one or more years of imprisonment. Section 193 of the Act further designates some countries that are parties to international Conventions with the UK will be able to make extradition requests for conduct provided in the specified Conventions. In addition, Section 194 allows arrangements for extradition from a country that does not have an extradition treaty with the UK. Lastly, now that the UK has left the EU, the UK is no longer a part of the European Arrest Warrant system. Extradition between the UK and EU is now governed by the EU-UK Trade and Cooperation Agreement.[223] When extradition is requested from the UK, several requirements must be met, including whether the conduct amounts to an offense in the requesting country.

218 The Agreement between the government of the United Kingdom of Great Britain and Northern Ireland and the government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crimes (3 October 2019) CP178
219 Convention against Transnational Organized Crime. https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html
220 Article 2(a) of the Convention against Transnational Organized Crime
221 Article 16 of the Convention against Transnational Organized Crime
222 The Extradition Act, 2003 (UK). https://www.legislation.gov.uk/ukpga/2003/41/contents
223 Section 29 of the European Union (Future Relationship) Act 2021 - provides that If arrested before 1 January 2021 the arrestee will be dealt with in terms of the European Arrest Warrant system.

Kenya

In Kenya, the Extradition (Commonwealth Countries) Act[224] governs extradition of persons to and from other Commonwealth countries. The alleged crime must be an offense in Kenya and the other country, the offense must fall within a description contained in the Schedule to the Act, and the law in the requesting country must punish the offense by at least 12 months in prison. OSEA offenses may fall into two categories of crimes listed in the Schedule; (1) Procuring or trafficking in women or young persons for immoral purposes (2) Blackmail or extortion by means of threats of abuse of authority.

In addition, any extradition request made to Kenya relating to an online sexual offense may be required to rely on crimes listed in the Sexual Offences Act and the Computer Misuse and Cybercrimes Act.

Nigeria

In terms of the Extradition Act, extradition of perpetrators to and from Nigeria is governed by individual treaties between Nigeria and other countries.[225] Nigeria is a party to the CRC Optional Protocol, therefore if Nigeria's extradition treaty with another Member State that has also ratified the CRC Optional Protocol refers to the relevant offenses in Article 3 of the CRC Optional Protocol, dual criminality will be deemed fulfilled.

US

The US relies on bilateral extradition treaties. It has entered into extradition treaties with more than 100 countries, including Kenya, Nigeria, the UK, and several EU Member States. Most of these rely on dual criminality. The remainder are "list treaties", which only provide for extradition in circumstances where a perpetrator has committed a crime listed in the relevant treaty. Relating to crimes against children, the US is also bound by the provisions of Articles 5 and 6 of the CRC Optional Protocol discussed above.

India

In India, the Extradition Act[226] provides the basis for extradition. India has signed extradition treaties with about 43 countries,[227] but none of the treaties expressly cover online offenses. The government of India may nevertheless have discretion to accept extradition requests for online offenses where the relevant extradition treaty contains a sweep-up clause authorizing the country to extradite for offenses that are not specifically listed. The extradition regime in India is also limited by the requirement for dual criminality. In addition, some of the extradition treaties bar the extradition of the signatory States' own nationals.[228] India has ratified the CRC Optional Protocol, and its provisions will apply in a similar manner as in the UK, US and Nigeria explained above.

Jurisdiction Over Companies

International human rights law generally imposes obligations on States, not on companies except in very limited circumstances.[229] It is up to States to regulate companies, within their jurisdiction, by prescribing their obligations through national laws.[230] At the national level, it is generally accepted that companies have legal obligations and may be held liable for infringing national laws, usually through fines. This framework generally applies to companies incorporated within the country or in cases where legal notices can be served on the company within that country.

There are essentially two ways that moderation of user-generated content on digital platforms is regulated at national level across the globe:

- Countries that adopt a strict liability approach where the digital service providers and platforms are treated as publishers and are required to actively monitor the content on their platforms, making them responsible for the user-generated content posted on the platforms.[231]
- Countries that treat digital service providers and platforms as mere conduits and afford them immunity from liability through "safe harbor" clauses in the law if they act within a reasonable time to remove illegal content when they become or are made aware of it.[232]

The regulation of digital service providers and platforms is discussed later in the report.

Technology companies are also operating across multiple jurisdictions, where their obligations under national law may differ and the provisions providing for OSEA, or lack thereof, also differ. These differences affect the recourse available to victims, depending on where they are located.

224 The Extradition (Commonwealth Countries) Act, 1968 (Kenya). http://www.vertic.org/media/National%20Legislation/Kenya/KE_Extradition_Commonwealth_Act.pdf
225 Extradition Act, 2004 (Nigeria). http://www.vertic.org/media/National%20Legislation/Nigeria/NG_Extradition_Act.pdf
226 Extradition Act 1962 (India). https://www.indiacode.nic.in/bitstream/123456789/1440/1/196234.pdf
227 https://mea.gov.in/leta.htm
228 https://www.ibanet.org/article/22AF1681-37A0-487A-A660-3ACA32938540
229 There are some internationally binding treaties that directly impose obligations on companies with regard to oil pollution and appropriation of the seabed or its minerals. See Art. III, International Convention on Civil Liability for Oil Pollution Damage (1969). See also Art. 137(1), UN Convention on the Law of the Sea (1982)
230 Clapham, A. (2002). 'The Question of Jurisdiction under International Criminal Law over Legal Persons: Lessons from the Rome Conference on an International Criminal Court', in Menno T. Kamminga and Saman Zia-Zarifi (eds.). Liability of Multinational Corporations under International Law. 139-195
231 https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability
232 http://rsrr.in/2020/10/21/safe-harbours-and-intermediary-liability/

Establishing Jurisdiction Over Digital Platforms
The Case of Pornhub

MindGeek owns and operates a complex network of over 100 sexually explicit websites, production companies, and brands including Pornhub. It is incorporated in Luxembourg, but operates out of Canada and has satellite offices in many other locations, including the US. Its subsidiary that does business as Pornhub is incorporated in Cyprus. The Pornhub website is available internationally and is the single largest website hosting sexually explicit content.

Several complaints have been made about Pornhub hosting and benefiting from OSEA. For instance, the Internet Watch Foundation reported having found 118 instances of CSAM, between 2017 and 2019.[233] Pornhub also has been described as a company which "monetizes child rapes, revenge pornography, spy cam videos of women showering, racist and misogynist content, and footage of women being asphyxiated in plastic bags."[234]

These complaints about Pornhub's activities have led to several civil suits filed against MindGeek, both in Canada and in the US. In 2020, MindGeek, was sued in California for Pornhub hosting videos created by GirlsDoPorn which trafficked women and girls and used "fraud, coercion and intimidation as part of its customary business practices to get women to film the videos."[235]

More recently, a group of plaintiffs from all over the world filed a class action lawsuit in California against MindGeek, its subsidiary doing business as Pornhub, other related companies, and several MindGeek owners and officers, including its CEO.[236] The plaintiffs brought the lawsuit under federal and state laws that prohibit human trafficking, racketeering, the sexual exploitation of children, and various tortious acts that cause harm.

To establish jurisdiction in California over defendants domiciled and incorporated primarily outside the US, the plaintiffs asserted that the defendants have offices and conduct business throughout the US, including in California. More specifically, the plaintiffs claimed that the defendants:

- Directed their activities at US citizens and California residents.
- Derived benefit from US citizens' and California residents' activities.
- Created a substantial connection with the US and the state of California.
- Engaged in significant activities in the US, including within California.
- Created continuing contractual obligations between MindGeek and US entities and citizens, including California citizens.
- Caused foreseeable harm to citizens in the US.[237]

At the time of writing, the court has not yet ruled on the case.

In addition, the Canadian House of Commons Ethics Committee launched an investigation into Pornhub and MindGeek. Its 2021 report made several recommendations, including that Canada's liability rules should be updated to make companies that host online pornography "legally accountable for content moderation and removal decisions and the harm to individuals that results when efforts are inadequate."[238]

The Canadian government stated that it will introduce legislation to create a new regulator that will ensure online platforms remove harmful content, including CSAM and intimate images shared without consent. Members of the Canadian government have also called on the Royal Canadian Mounted Police to launch a full criminal investigation into MindGeek based on the activities of Pornhub.[239]

233 https://www.bbc.com/news/world-52543508
234 https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html
235 https://nypost.com/2020/12/16/pornhub-owner-sued-for-profiting-off-sex-trafficking-court-papers/
236 The Defendants are MindGeek S.a.r.l.; MG Freesites, Ltd. d/b/a Pornhub ("Pornhub"); MindGeek USA Incorporated ("MindGeek USA"); MG Premium Ltd.; RK Holdings USA Inc.; MG Global Entertainment Inc.; TrafficJunky Inc. d/b/a Trafficjunky.com (collectively "MindGeek"); Bernd Bergmair; Feras Antoon; David Tassillo; Corey Urman; Bernd Bergmair; and Colbeck Capital Management LLC (MindGeek together with Bergmair, Antoon, Tassilllo, and Urman, Bergmair, and Colbeck Capital the "MindGeek Defendants"); and Visa Inc.
237 https://brownrudnick.com/wp-content/uploads/2021/06/2021.06.17-Dkt.-001-Complaint.pdf
238 https://www.politico.com/news/2021/06/17/canadian-committee-tough-action-pornhub-495077
239 https://www.cbc.ca/news/politics/regulator-online-sexual-exploitation-1.5984433

Establishing jurisdiction of a company operating and providing services across multiple countries presents a challenge for victims in many countries when they want to seek justice against these companies. Challenges also arise where national laws treat digital service providers and platforms as mere conduits, and they are not legally liable for harmful user-generated content where they are not reasonably aware of it.

The proposed UN Business and Human Rights Treaty, currently in its third draft, attempts to address some of these challenges by providing some clarification on actions that governments can take. It seeks to "clarify and facilitate the effective implementation of States' obligation to respect, protect and promote human rights in the context of business activities, as well as the responsibilities of business enterprises, no matter the size or reach of the enterprise… to prevent the occurrence of human rights abuses… in this context,… to ensure access to justice and effective remedy for victims and facilitate and strengthen mutual legal assistance and international cooperation to prevent human rights abuses in the context of business activities".[240] The draft Treaty also requires States to avoid placing cumbersome legal obstacles to obtaining justice, such as those around the establishment of jurisdiction.[241] The draft Treaty also calls for States to pay "special attention to both gender-based and sexual violence."[242]

Challenges and Gaps Around Jurisdiction

The current international legal framework has challenges and gaps that make it difficult to prosecute offenses. For example, the framework:

- Does not fully cater to all groups affected by OSEA.
- Has limited scope for international cooperation between and among countries.
- Requires dual criminality.
- Is hampered by challenges in identifying and collecting digital evidence from cloud storage.

Gaps in Groups Affected by OSEA

The current international legal instruments that provide specifically for establishing jurisdiction in relation to sexual offenses, territorial and extraterritorial, are important in creating a common standard across countries. They include:

- The Budapest Convention, ratified by 64 countries.
- The Lanzarote Convention, ratified by 45 countries.
- The CRC Optional Protocol, ratified by 121 countries.

These instruments, however, have limited applicability. They relate only to sexual offenses against children, but do not adequately address all forms of OSEA against children. Also, there are no international frameworks that relate specifically to OSEA against adults.

Limited Scope for International Cooperation

The framework established under the three international instruments largely relies on cooperation between States, which is in turn dependent on whether the relevant States have ratified the same instrument. Any country that has not ratified any of the instruments at issue has to rely on its national law to make requests for assistance or to comply with requests from other countries. This gap illustrates a potential area of weakness in prosecuting offenses.

Because of the low ratification rate of both the Budapest Convention and the Lanzarote Convention, there is no legal obligation for the majority of countries to cooperate with each other when handling multi-jurisdictional crimes that are established in the two Conventions.

Establishing jurisdiction of a company operating and providing services across multiple countries presents a challenge for victims in many countries when they want to seek justice against these companies. Challenges also arise where national laws treat digital service providers and platforms as mere conduits and they are not legally liable for harmful user-generated content where they are not reasonably aware of it.

240 Article 2 of the Third Draft of the Business and Human Rights Treaty 2021. https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/Session6/LBI3rdDRAFT.pdf
241 Article 9 of the Third Draft of the Business and Human Rights Treaty
242 Article 16.3 of the Third Draft of the Business and Human Rights Treaty

Radhika - India
Survivor Story

I set up a Facebook profile and received a friend request from a man I didn't know. I saw a few of my family were connected with him so I accepted. He got my telephone number from somewhere and messaged me on WhatsApp.

He asked about my family and I told him I was still with my husband. My parents had four daughters and arranged for me to marry when I was ten years old to ease their financial burden. After a few years, my husband married another woman and I moved with my two sons to live with my parents.

He made inquiries to others and found out I was a divorcee. He told me he was also divorced and that he liked me, my voice, and my photos on Facebook. A few days later, he called again to say he was in love with me. I told him that I imagined my future partner as someone who'd love my children but I wasn't looking for a husband because I was happy with my sons. But despite my refusal, he kept calling. Eventually, as I thought we were from the same caste, I decided to talk with my sisters and they said I should consider his proposal because it would be better than being alone and he could look after me.

So I told him I wanted to get married, not just be in a relationship. He agreed and made several oaths so I'd trust him. In secret, he gave me a mangala sutra (a necklace that a groom ties around a bride's neck) and said now we are married. I refused and said I wanted a legal marriage, not a false one.

He took me to his sister's place and the first night I slept alone without trouble. He told me he talked with a lawyer and we went to the court and some temples but we did not see a lawyer or a priest.

He promised we'd get married the next day and on the second night, he entered my room. He started getting close and I resisted but it was no use. I shouted for help and his sister and her husband entered the room and tried to convince me to go ahead as we were getting married. Then they locked the door and he raped me.

In the morning, he dropped me at the roadside and switched off his phone. I tried calling many times and walked 20 kilometres home. I told my mother I was going to file a police complaint. She opposed this as she was concerned that our community would find out and it would bring me more trouble. But still, I decided to lodge the complaint because I felt he could do the same thing to other girls.

First, I went to my local police station but was told that as the crime was committed elsewhere, the case could only be lodged in that area. So I travelled to where the assault happened and again attempted to file my complaint against him, his sister, and brother-in-law.

The accused and his family tried to convince me not to go ahead and said he was ready to marry me. His parents spoke with the police and the police remained unwilling to accept my complaint. Eventually, they agreed but did not note down everything I said. I had phone recordings which strengthened my case but they refused to accept my evidence. The next day, I had to return to the station and speak with another officer, who made me repeat all the details again. His family offered money but I refused. His father also told people in my village and requested they talk to me. A few tried to force me to withdraw my case and kept coming to pressure me.

Months have passed and I have literally begged the police to take the voice recording which establishes the truth but they are not responding and I cannot afford to keep travelling to the station.

My mental state is very poor. Such an incident lives with you forever and the stigma never goes away. Now, I think "never believe what people tell you". I feel like it is a sin to be a woman and only those with money and power get justice.

"First, I went to my local police station but was told that as the crime was committed elsewhere, the case could only be lodged in that area. So I travelled to where the assault happened and again attempted to file my complaint against him, his sister, and brother-in-law."

Dual Criminality

Extradition of perpetrators typically depends on the principle of dual criminality, meaning that an offense must be recognized as an offense in the nation where it was committed as well as the nation where it would be prosecuted. This requirement can hinder extradition because the country requesting extradition needs to prove that the individual's action is also an offense in the requested country.[243]

The dual criminality requirement can be more easily met if both of the countries in question have ratified a Convention or Protocol which prohibits the offense at issue. However, if one of the countries is not a signatory, the Convention or Protocol does not offer any extradition advantage. For example, Kenyan law requires dual criminality for extradition, but Kenya is not a signatory to the CRC Optional Protocol. Therefore, dual criminality is not deemed to be fulfilled simply because the offense is one listed under Article 3 of the CRC Optional Protocol. If dual criminality cannot otherwise be established, Kenya would have to rely on an extradition treaty. A treaty like the UN Convention Against Transnational Organized Crime might suffice, but the alleged crime would have to be punishable by at least a four-year sentence.

Other international treaties whose provisions enable international cooperation to still occur without a strict interpretation of the dual criminality requirement may provide a valuable model going forward. For example, Article 43(2) of the UN Convention Against Corruption provides that, "whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offense within the same category of offense or denominate the offense by the same terminology as the requesting State Party, if the conduct underlying the offense for which assistance is sought is a criminal offense under the laws of both States Parties."[244] This principle could be considered when governments develop international standards that address OSEA crimes.

Identification and Collection of Digital Evidence

Even with international cooperation mechanisms in place, challenges may arise in the identification and collection of digital evidence across jurisdictions. Cloud computing poses a particular challenge because cloud data can be fragmented and stored across multiple locations and multiple countries.[245] It becomes difficult to determine under which jurisdiction the data is stored and whether digital evidence can be gathered extraterritorially.

The US case, ***US v. Microsoft Corporation***, illustrates the challenges posed by cloud storage.[246] Federal agents obtained an 18 U.S.C. 2703 warrant pursuant to the US Stored Communications Act (SCA) requiring Microsoft to disclose all emails and other information associated with a customer's

...challenges may arise in the identification and collection of digital evidence across jurisdictions. Cloud computing poses a particular challenge because cloud data can be fragmented and stored across multiple locations and multiple countries.

243 Jonathan O. Hafen, International Extradition: Issues Arising Under the Dual Criminality Requirement, 1992 BYU L. Rev. 191 (1992). https://digitalcommons.law.byu.edu/lawreview/vol1992/iss1/4

244 https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

245 https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/challenges-relating-to-extraterritorial-evidence.html

246 *United States v. Microsoft Corp.*, 138 S. Ct. 1186, 200 L. Ed. 2d 610 (2018). https://casetext.com/case/united-states-v-microsoft-corp-9

Unsplash/Andras Vas

account that was believed to be involved in drug trafficking. Microsoft handed over relevant non-content data stored on US servers (for example, the suspect's address book) but did not give the US government relevant content data (for example, content of the individual's emails) that was stored at Microsoft's data center in Ireland. It was unclear whether the SCA applied extraterritorially. While the case was pending, Congress passed the CLOUD Act, which requires internet companies to hand over personal data to US law enforcement agencies under the SCA no matter where that data is stored. In the absence of international provisions that deal with collection of digital evidence, governments must rely on their national laws resulting in inconsistent practices across the world.

Conclusion

The current international legal framework for establishing jurisdiction and cooperation among States presents some opportunities for prosecution of OSEA crimes but also leaves some significant gaps. The framework needs to be updated to take into account the complexities of digital technology and the range of OSEA crimes. Governments must update their national laws to account for all forms of OSEA crimes and to ensure their laws support the international framework.

DIGITAL RIGHTS AND OSEA

A well-functioning internet needs to be based on respect for users' right to freedom of expression. Any restrictions on freedom of expression must be lawful and tailored as specifically as possible. The right to privacy is another pillar of a well-functioning internet. This right includes the protection of personal information and respect for the confidentiality of communications.[247] Alongside the right to privacy and freedom of expression, everyone is entitled to protection from harm. In practice, tensions arise between these rights. Fundamental questions arise on how these competing rights should be balanced in law and practice. These issues also apply to digital service providers and platforms in how they detect and remove sexual abuse and exploitation content from their platforms.

Freedom of Expression Online and OSEA

The right to freedom of expression is enshrined in various international legal instruments. For example, the Universal Declaration of Human Rights provides that, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[248] The ICCPR provides similar protection.[249] This right has been incorporated into most regional and national laws. It is considered to be a cornerstone right of a democratic society.

247 Council of Europe, Privacy and Data Protection. https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection
248 Article 19 of the Universal Declaration of Human Rights 1948
249 Article 19 of the International Covenant on Civil and Political Rights.

Balancing Freedom of Expression Against Safety and Protection from OSEA

Online activities are considered expression and enjoy protection under the right of freedom of expression. However, some activities are harmful and infringe on the rights and safety of others. The ICCPR provides a framework for limiting freedom of expression to protect the rights and reputation of others, national security, and public order, health, and morals.[250] These limited, permissible restrictions on freedom of expression can be found in many regional laws and national constitutions. For example:

- Article 13 of the American Convention on Human Rights provides that the right to freedom of expression can be "limited by law to the extent necessary to protect the rights and reputation of others."[251] It specifically provides that the production, consumption, and distribution of CSAM is not protected by freedom of expression.

Online activities are considered expression and enjoy protection under the right of freedom of expression. However, some activities are harmful and infringe on the rights and safety of others.

- The African Charter on Human and People's Right provides that everyone has the right to receive information and the right to express and disseminate one's opinion "within the law".[252]
- Paragraph 16 of the EU Guidelines on Freedom of Expression Online and Offline acknowledges that the internet and digital technologies have expanded the possibilities of individuals and media to exercise the right to freedom of expression and freely access online information. The Guidelines highlight that any restriction that "prevents the flow of information offline or online must be in line with permissible limitations as set out in international human rights law".

The framework for limiting freedom of expression in these instances is commonly referred to as the proportionality test. To satisfy this test under the ICCPR framework, a restriction must be:

- Legal, meaning the law is clear and unambiguous.
- Legitimate, designed to protect individual rights and public concerns.
- Reasonable, meaning the restriction is necessary to protect legitimate rights but narrowly drawn to address the objective, meaning a fair balance is struck between protecting fundamental rights and the interests of the community.

Under this test, national courts determine on a case-by-case basis whether any limitation imposed on freedom of expression is legal, necessary, and proportionate. Digital platforms also similarly balance between freedom of expression and protection from OSEA in their content moderation, and they make decisions on whether to limit freedom of expression in order to protect people from OSEA on their respective platforms.

Many courts in various jurisdictions have applied the proportionality test to prohibitions on CSAM and some other forms of OSEA.

The Restrictions Must Be Legal

Laws restricting a fundamental right, like freedom of expression, must be clear, unambiguous, and address an area of legitimate public concern. Governments must not have unfettered discretion to restrict the right of freedom of expression.[253]

In the focus countries, there are some examples where criminal laws impose legal limitations on the right to freedom of expression in relation to sexual crimes. The examples show that governments have tended to place greater emphasis on protecting children from exploitation and abuse.

In the US, First Amendment constitutional rights of freedom of speech and expression exclude offers or requests to obtain CSAM from freedom of expression protections.[254] Similarly, in the UK, the right to freedom of expression under Article 10(1) European Convention on Human Rights is limited by criminal provisions contained in the Obscene Publications Act.[255] In Kenya, laws that protect from sexual exploitation and abuse and criminalize the production and possession of CSAM, such as the Sexual Offences Act,[256] the Children Act,[257] the Penal Code,[258] and the Computer Misuse and Cybercrimes Act,[259] have provisions that limit the right to freedom of expression on the basis of protecting children from abuse and exploitation.

250 Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR) states that the exercise of freedom of expressions comes with "special duties and responsibilities" and therefore can be limited provided the restrictions "shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."
251 Article 13 of the American Convention on Human Rights, 1969. https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf
252 Article 9 of the African Charter on Human and People's Right
253 Paragraph 24 of the ICCPR General Comment 34 (2011) on Article 19 on Freedom of opinion and expression
254 *United States v. Williams*, 553 U.S. 285, 299 (2008)
255 The Crown Prosecution Service, Obscene Publications (rev. January 2019), available at https://www.cps.gov.uk/legal-guidance/obscene-publications
256 Section 16A of the Sexual Offences Act (Kenya)
257 Section 15 of the Children Act (Kenya)
258 Section 238 of the Penal Code (Kenya)
259 Section 24 of the Computer Misuse and Cybercrimes Act (Kenya)

Criminal provisions in India's Penal Code and the Protection of Children from Sexual Offences Act[260] also limit offenders' right to freedom of expression on the basis of protecting children from abuse through CSAM, grooming, and communicating with a child with the intention of promoting sexual exploitation. Similarly, Nigeria's Cybercrimes (Prevention, Protection, etc.) Act also imposes limits on freedom of expression through provisions that prohibit online grooming of children and CSAM.[261]

The legality element requires that the laws are clear and not vague, an issue addressed by the US Supreme Court in ***Ashcroft v. Free Speech Coalition***.[262] ***Ashcroft*** addressed whether the Child Pornography Prevention Act of 1996 (CPPA) lawfully abridged freedom of speech. CPPA was drafted broadly to prohibit CSAM, and the prohibitions extended to sexually explicit images that appeared to depict minors but were produced without using any real children. The Supreme Court held CCPA to be overbroad and unconstitutional as its breadth and ambiguity were overreaching. In response to the Supreme Court's opinion in ***Ashcroft***, the US government had to clarify the ambiguity in the law, which led to the enactment of the Protect Act.[263] The Protect Act provides that the depiction of actual children, although necessary for sexual exploitation statutes, is not necessary for obscenity statutes.

The Restriction Must be Legitimate, Protecting Important Individual Rights and Areas of Public Concern

Respect for the rights and reputations of others provide the framework for legitimate grounds for restricting freedom of expression in the context of online sexual crimes. Given the extent of the harms (emotional, psychological, physical, and at times financial) that women, girls, and children experience as a result of OSEA, it can be argued that acts of OSEA cannot be protected under the right to freedom of expression.

The ICCPR also provides that freedom of expression may be restricted for the protection of public morals. ICCPR Committee in its General Comment 34 (2011) on Article 19 on the right to freedom of expression observed that "the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations... for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition".[264]

The concept of public morals has been used in a number of national laws, including in Kenya, the UK, and the US to criminalize content that is deemed to be obscene. In determining whether an action is against public morality and is obscene, courts in the UK and the US have tended to consider the perception of an ordinary person on the

REUTERS/Kyle Grillot

260 Sections 11, 13 and 15 of the Protection of Children from Sexual Offences Act, 2012
261 Section 23(3) of the Cybercrimes Act (Nigeria)
262 *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002). https://www.law.cornell.edu/supct/html/00-795.ZO.html
263 The Protect Act, 2003 (US). https://www.congress.gov/bill/108th-congress/senate-bill/151
264 Paragraph 32 of ICCPR General Comment 34 (2011).

offensiveness and severity of the action. Thus, what is obscene is determined by the moral standards of the community at the time the case is being determined.

Under the UK's Obscene Publications Act, the court in ***Handyside v. UK*** considered whether a book aimed at children aged 12 and over might encourage them to "indulge in precocious activities harmful for them or even to commit certain criminal offences" which would be in breach of the Obscene Publications Act. The court suggested the requirements of morals vary from time to time and from place to place and that national law enforcement were therefore best placed to judge what was needed.

In the US, the Supreme Court established the Miller Test[265] that judges and juries use to determine whether material is obscene. The test relies heavily on the perception of the ordinary person on the street, whether the ordinary person, being of sound and reasonable mind, would find the material went against the moral standards of their community.

Although the concept of public morals can be used to criminalize OSEA material and content particularly related to children, it is fraught with challenges. In some countries it has been used to police and criminalize women's social behavior, particularly in instances where women consensually generate and share content that is seen as an "expression of female sexuality."[266] The concept of public morals should not be used to suppress women's freedom of expression and in its application courts should "consider the universality of human rights and principles of non-discrimination".[267]

The Restrictions Must be Reasonable, Striking a Balance Between the Competing Interests

Specifically relating to OSEA, the question of whether a law is proportionate and narrowly drafted has arisen in the case of the FOSTA-SESTA law in the US which amends Section 230 of the CDA. Section 230 immunizes websites and other online service providers from liability for the actions of their users on their services with only a few exceptions. FOSTA-SESTA eliminates immunity for service providers that knowingly participate in and support the facilitation of sex trafficking.

A constitutional legal challenge has been brought against FOSTA-SESTA (which is still pending) on the grounds that the law abridges the First Amendment right to free speech.[268] The plaintiffs argue that by amending Section 230 of the CDA, FOSTA-SESTA expansively criminalizes online speech related to prostitution and removes important protections for online intermediaries in violation of their First Amendment rights.[269] The Woodhull Freedom Foundation, which brought the case together with Human Rights Watch and two other plaintiffs, argues "the law is undefined and vague terms can sweep up constitutionally protected speech and potentially lead to… criminal prosecution, as well as civil liability".[270]

Those supporting the law argue that it is proportionate because it narrowly specifies the grounds on which immunity is removed, specifically when websites knowingly facilitate sex trafficking and prostitution on their platform such as through online ads. It intends to end situations where Section 230 of the CDA shielded a number of websites, such as classified ads website Backpage.com, from prosecution and prevented victims of sex trafficking from having any legal recourse against these websites. A Senate investigation found Backpage.com actively engaged in the editing of prostitution-related ads with knowledge of facilitating sex trafficking.[271] Reports also indicate that companies like Backpage, which was the hub of online sex trafficking in the US at the time FOSTA-SESTA was passed, reaped $500 million in profits from ads promoting sex trafficking and sexual exploitation.[272] Given the exploitation and harm perpetrated against people exploited on these sites, primarily women and girls, it is reasonable to conclude that FOSTA-SESTA is necessary and legitimate, but the US courts have yet to determine whether it is drawn narrowly enough to survive the proportionality test.

Privacy Online and OSEA

The right to privacy protects individuals from intrusion into their own or their family's personal life by third parties. Article 12 of the Universal Declaration of Human Rights defines the right to privacy as the right to protection of the law against "arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[273] The ICCPR provides similar protection.[274]

The right to privacy has also been enshrined in many regional and national laws. For instance, the EU General Data Protection Regulation (GDPR) provides for protection of personal data in the EU and European Economic Area (EEA). In addition, the Privacy and Electronic Communications Directive (e-Privacy Directive) more specifically provides for the confidentiality of communications and the rules regarding tracking and monitoring of electronic

265 *Miller v. California*, 413 U.S. 15 (1973) (US). https://www.thefire.org/first-amendment-library/decision/miller-v-california/
266 Report on Gender Justice and Freedom of Opinion and Expression. At Para 24. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/212/16/PDF/N2121216.pdf?OpenElement
267 *Miller v. California*, 413 U.S. 15 (1973)
268 See *Woodhull Freedom Found. v. United States*, No. 18-5298, 2020 WL 398625 (D.C. Cir. Jan. 24, 2020).
269 Halverson,H. (2018). The Communications Decency Act: Immunity for Internet-Facilitated Commercial Sexual Exploitation," *Dignity: A Journal of Analysis of Exploitation and Violence: Vol. 3: Iss. 1, Article 12*. DOI: 10.23860/dignity.2018.03.01.12
270 https://www.eff.org/press/releases/victory-lawsuit-challenging-FOSTA-SESTA-reinstated-court
271 US Senate, Backpage.com's Knowing Facilitation of Online Sex Trafficking, Hearing before the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs, 2017. https://www.govinfo.gov/content/pkg/CHRG-115shrg24401/html/CHRG-115shrg24401.htm
272 https://www.wired.com/story/inside-backpage-vicious-battle-feds/
273 Article of the Universal Declaration of Human Rights 1948.
274 Article 17 of the International Covenant on Civil and Political Rights, 1976. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

communications in the EU and EEA. The GDPR and the e-Privacy Directive provide for privacy while online and call on Member States to ensure transparency, confidentiality, accountability, and security of personal data and online communications.

Balancing Privacy Online Against Safety and Protection from OSEA

Internet users have a reasonable expectation of privacy while online but protecting that privacy can lead to conflicting results. On the one hand, that expectation of privacy can protect users from sexual exploitation and abuse, such as having their personal and sexual information shared and distributed without their consent. On the other hand, that privacy provides a level of anonymity which perpetrators have taken advantage of to sexually exploit and abuse with impunity.

The Right to Privacy As a Means to Protect Victims of OSEA

The right to privacy and data protection protects individuals from criminal or harmful activities relating to their sexual and personal information. Individuals are supposed to have control over their information and if, when, how, and with whom this information in different forms (like images, audio, and text) is produced and shared online. Consequently, in the event that the material is shared or published without the individual's consent, digital service providers and platforms should remove the material and report the incident to law enforcement. For example, in Kenya, in the absence of a specific law criminalizing image-based sexual abuse, victims can bring civil suits involving infringement of privacy and copyright,[275] and intentional infliction of emotional distress.

Another way privacy laws can be used to protect individuals is through invoking the right to be forgotten. For example, Europe recognizes the right to be forgotten as a corollary to the right to privacy provided for in Article 17 of the GDPR and that right is well-established in Europe's jurisprudence. It involves the right to have personal data erased under certain circumstances. The GDPR recognizes that asserting the right to be forgotten (or the right to erasure) may directly compete with the exercise of the right of freedom of expression and information. However, in the context of OSEA, where data is illegally produced or obtained, retained, or disseminated, it is difficult to argue that freedom of expression of an alleged perpetrator should prevail over the right to have such data removed.

Limiting the Right to Privacy in the Context of OSEA

Anonymity online can create opportunities for perpetrators to hide their identity and information about their location, which are both necessary to bring them to justice. Across the focus countries, the right to privacy of an alleged perpetrator is limited to allow for criminal investigations and prosecutions. The proportionality test discussed earlier is also relevant when seeking to limit the right to privacy in these instances.[276]

Europe

The Court of Justice of the European Union (CJEU)[277] ruled the e-Privacy Directive "must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication". The court emphasized that access by competent national authorities to the retained data is to be restricted solely to fighting "serious crime", and that the data must be retained within the EU. However, a main challenge is that "serious crime" is defined differently by each Member State.

US

In the US, the Stored Communications Act (SCA) sets forth the procedures by which law enforcement can compel digital service providers to disclose the contents of and other records pertaining to user accounts. This law applies to email accounts as well as social media, cloud storage, web-hosting accounts, and any other type of account where a user may store electronic communications. The courts have generally upheld the constitutionality of law enforcement's access to online information via the mechanisms provided by the SCA.

India

Similar to the US, India's IT Act Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules[278] does not require prior consent to share information with government agencies mandated to obtain information (including sensitive personal data) for verifying one's identity and for the prevention, detection, investigation, prosecution, and punishment of offenses.[279]

Kenya

In Kenya, the Data Protection Act lists exceptions allowing publication of private data, where it would be in the public interest, for journalism, literature and art, research, history, and statistics, as prescribed by the Data Commissioner. The Act envisions that the Commissioner

275 Under Kenya's Copyright Act, they would have to establish authorship of the images.

276 European Data Protection Supervisor (2019) Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf

277 *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203

278 In India there is no specific laws for protection of Data, the privacy and protection of Data are governed by the IT Act Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules)

279 Rule 6(1) of the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011

would ensure adherence to codes of ethics in approving such exemptions.[280] This flexibility provides an opportunity for the Commissioner to designate the publication of private data in the pursuit of criminal investigations relating to OSEA crimes as a permissible exception.

Nigeria

The Nigerian Data Protection Regulation (NDPR) permits disclosure of personal data to law enforcement agencies where there is a lawful basis for processing such data (including for the fulfilment of a legal obligation by the data subject) and for the protection of the interests of another person. Protection from OSEA could potentially be a legitimate reason under the "protection of the interest of another person" requirement. Further, the NDPR permits the transfer of personal data to foreign countries under certain conditions including where the data subject is answerable in a duly established legal action for any civil or criminal claim in a third country. This permitted transfer would potentially be applicable in civil and criminal cases arising from OSEA.

Encryption, Privacy, and Protection from OSEA

The move by digital technology companies towards stronger encryption on their platforms, on the basis that this approach would increase privacy and data protection, poses a particular challenge. Encryption offers many benefits, such as:

- Being a secure technology intended to keep people safe and protect their digital rights.
- Protecting some of the most important digital information, like details about health, finances, relationships, family, and political views, from exploitation and surveillance.
- Enabling everyone, from children attending school online to journalists and whistleblowers, to lawfully express themselves online and access information without fear of retribution.

However, the move towards stronger encryption poses a challenge to detecting OSEA that potentially enables offenders to hide criminal activity, shield themselves from detection, and continue to operate with impunity. For example, Facebook Messenger and WhatsApp have started to use end-to-end encryption that allows only the sender and receiver to access the message. The two online platforms do not have access to the message with this form of encryption making it theoretically impossible for the platforms to hand over decrypted messages to law enforcement authorities. Also, even if a platform does hand over this type of encrypted messages, it would take law enforcement considerable time to decrypt the messages, potentially giving the perpetrators time to evade detection. Therefore, end-to-end encryption on messaging platforms has been criticized because the blanket privacy coverage can conceal crimes.

An increasing global consensus has begun to recognize that although encryption is vital, and privacy and cyber security must be protected, these interests should not come at the expense of precluding law enforcement and the technology industry from acting against illegal content and activity. In 2019, the UK, the US, Australia, New Zealand, and Canada issued a communique, concluding that "tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can gain access to data in a readable and usable format. Those companies should also embed the safety of their users in their system designs, enabling them to take action against illegal content."[281]

On the other hand, proponents of continuing strong encryption have argued that the calls to curtail end-to-end encryption are a move that would infringe on users' privacy and would result in self-censorship consequently abridging freedom of expression. This viewpoint is based on the argument that if internet traffic is unencrypted, "any government, company, or criminal that happens to notice it can – and, in fact, does – steal a copy of it, secretly recording your information forever".[282] Moreover, the proponents argue that encryption provides a secure means of communication for activists and whistleblowers; disabling encryption or allowing governments to have private encryption keys could put them in jeopardy.

Directly related to OSEA, these concerns surfaced following the introduction in the US Senate of the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT) in 2020.[283] EARN IT proposed to amend Section 230 of the CDA to completely eliminate service providers' immunity for CSAM posted by users.[284] Civil liberties supporters argued that limiting the Section 230 immunity of technology companies would result in a curtailing of encryption and consequently unduly limit freedom of expression and privacy online. Although this bill died in the 2020 Congress, the arguments raised after its introduction illustrate the conflicting opinions around encryption.

280 Kenya Data Protection Act, Part VII.

281 See International Statement, End to End Encryption and public safety. https://www.gov.uk/country/publications/international-statement-end-to-end-encryption-and-public-safety/international-statement-end-to-end-encryption-and-public-safety-accessible-version

282 Edward Snowden. (2019, October). Without encryption, we will lose all privacy. This is our new battleground. The Guardian. https://www.theguardian.com/commentisfree/2019/oct/15/encryption-lose-privacy-us-uk-australia-facebook

283 Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, 2020. (US) https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

284 Pfefferkorn, R (2020, June). (2020, June). There's Now An Even Worse Anti-Encryption Bill Than EARN IT. That Doesn't Make The EARN IT Bill Ok. The Center for Internet and Society at Stanford Law School. http://cyberlaw.stanford.edu/blog/2020/06/there's-now-even-worse-anti-encryption-bill-earn-it-doesn't-make-earn-it-bill-ok

Gibi - US
Survivor Story

Gibi's interview was shared with Equality Now through #MyImageMyChoice, a survivor-led coalition asking for trauma-informed global laws and policy on intimate image abuse.

Gibi is an Autonomous Sensory Meridian Response (ASMR) artist and Youtuber who has around 3.8 million subscribers for her ASMR focused YouTube channel.

My deepfakes have been around ever since I started my YouTube channel. I've seen how it has gotten very good so that makes me extremely nervous because I know how fast technology can advance. When I first saw a deepfake, I was reading about how the computer learns and gets better at matching your face and putting it onto something pornographic. Watching the videos is very surreal - people believe it's real.

The thing that bothers me is I did not consent for my image to be used that way, they are able to do it with no consequences and it feels very violating. I contemplated deleting my channel because I felt very overwhelmed by these people that I didn't know that seemed to want to hurt me, to make me feel horrible, violate my privacy, and feel power over me. But it's something that I just keep working through and I do my best to protect my privacy.

Do I ever feel safe? Not really! It started very early on, I had barely any following and I learned my lesson quickly. They figured out my real name, where I lived, who my family was, where I went to school, and they posted it everywhere.

I have been very paranoid, nervous, fearful, and have had a few bad anxiety attacks in public when I thought I might be unsafe. I'm thinking about it constantly - making sure that you don't slip up, that people don't know where you are, you can't let people know your family. It's a way of life now but I would never say that I feel safe on the internet, ever.

I used to keep tabs on the deepfakes until it felt useless, if you let it consume you it's gonna waste your time and that's not what I want. They will make more and more of me and it doesn't do me any good to watch them, so I've stopped for my own sanity.

I don't seek them out but I try to keep tabs on what's being posted about me across the internet. I'm trying to do my daily job so I'll end up in an anonymous forum or random page, and porn of me is littered in with that. Sometimes people will email them to me, like "Gibi, somebody made porn of you!"

I get why people watch, they think it's victimless. But obviously I don't want people to see it, and if there's less demand there would be less videos. One time I saw somebody was doing commissions, making money off my doctored photos and videos. They're running this business, profiting off of my face doing something that I didn't consent to, like my suffering is your livelihood. It made me really mad, but again, there was nothing I could do so I just had to leave it.

I was approached by a company taking deepfakes off the internet. I'm like "Oh, great!" And they sent me their prices and its exorbitant, $600 to take a video off a deepfake website. Why should I be using my hard earned money to be paying you to privately take down these videos?

I think that lawmakers and governments are extremely overwhelmed by the internet so they just let it go. If somebody's making a deepfake in a different country, my country doesn't care because there's nothing they can do. I can't think of a single organization equipped to deal with this, and that's why it feels very helpless.

For me, justice would be not letting them be anonymous anymore. It's much too easy to make yourself anonymous online where law enforcement doesn't care enough to put in the effort to find out who's doing it. I would like to know who is making pornographic content from my own face. They know me. OK, what's your name? Where do you work? It just seems very unbalanced and unfair right now.

Being a woman on the internet is hard because of the lack of policing, the lack of laws. Putting yourself on the internet means you're not protected. It's a choice I wish that I didn't have to make - that if I want to continue my career. If somebody asks, "Hey I want to be a YouTuber!" it sucks that I have to tell them "you need to protect yourself because people will come after you, because this is part of the job." And I hate that it's part of the job, it's disturbing and it shouldn't be OK.

The Role of Digital Companies in Balancing Freedom of Expression, Privacy, and the Right to Protection and Safety

Courts have historically applied the proportionality test and balanced between competing rights and interests.[285] However, many digital service providers and platforms are moderating user content online and making decisions that balance freedom of expression, privacy, and the right to protection and safety.

A 2018, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression report[286] recommended that information and communication technologies use human rights principles to moderate user content. The report also stated that the human rights principles, if implemented transparently and consistently with meaningful civil society input, could provide a framework to hold States and companies accountable to users across national borders.[287] Furthermore, by adopting human rights principles in their practices, including in content moderation, companies could create an environment that accommodates the needs of users while establishing predictable and consistent baseline standards of behavior.[288] The report emphasized that human rights principles would offer a globally recognized framework for companies to design tools to address harms, such as misogynistic or homophobic harassment designed to silence women and sexual minorities. The principles would also provide a common vocabulary to explain their nature, purpose, and how they apply to users and governments. The report's recommendation for a human rights-based approach to content moderation would be well-suited for companies seeking common norms across various jurisdictions rather than relying on a patchwork of national laws.[289]

The call for digital service providers and platforms to apply human rights principles in content moderation can also be gleaned from the UN Guiding Principles on Business and Human Rights (Guiding Principles).[290] The non-binding Guiding Principles provide that businesses should:

- Avoid causing or contributing to adverse impacts on human rights.
- Address these impacts when they occur.
- Prevent or mitigate adverse impacts on human rights that are directly related to their operations, products, or services by their business relationships, even if they have not contributed to those impacts.

Moreover, the International Bill of Human Rights,[291] which is referred to in the Guiding Principles, states that gender-based violence and all forms of sexual harassment and exploitation are incompatible with human dignity. The proposed Business and Human Rights Treaty would place obligations on national governments to hold businesses accountable for human rights infringements and abuses, including gender-based and sexual violence.[292]

Conclusion

The mechanisms for balancing freedom of expression, privacy, and safety and protection from online harms provide some opportunities but are also fraught with many challenges. A key opportunity is the principle, established under international law, that in the event of a crime, privacy and freedom of expression of alleged offenders can be limited if the limitations are legal, legitimate, necessary, and proportionate. The challenge is that there must be adequate laws that criminalize OSEA in its various forms, and legal clarity is required to define what constitutes OSEA. In addition, legal clarity on the relationship between freedom of expression, privacy, and online violence and harms towards women is specifically required. This approach would be similar to instances where States categorically exclude offers or requests to obtain CSAM from freedom of expression protections.

Digital service providers and platforms have a significant role in balancing competing rights in content moderation. The UN Special Rapporteur report's recommendation, echoed in the Guiding Principles, that these entities adopt a human rights-based approach to content moderation would ensure consistency and incorporate gender equality.

285 Sobek T., Montag J. (2018) Proportionality Test. In: Marciano A., Ramello G. (eds) Encyclopedia of Law and Economics. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-7883-6_721-1

286 United Nations Human Rights Commission (UNHRC) Report on Online Content Regulations by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://www.undocs.org/A/HRC/38/35

287 Paragraph 41 of the United Nations Human Rights Commission (UNHRC) Report on Online Content Regulations by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression available at https://www.undocs.org/A/HRC/38/35

288 Ibid. Note 283 at Para 43

289 Ibid. Note 283

290 United Nations Human Rights Office of the High Commissioner. (2011). Guiding Principles on Business and Human Rights. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

291 The International Bill of Rights consists of the Universal Declaration of Human Rights and the main instruments through which it has been codified: the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights), coupled with the principles concerning fundamental rights in the eight ILO core conventions as set out in the Declaration on Fundamental Principles and Rights at Work

292 Article 16 of the Third Draft of the Business and Human Rights Treaty 2020

Mohamed Daghar
Expert Interview

Regional Coordinator
Eastern Africa: Enhancing Africa's response to transnational organized crime - Kenya

"Kenya is a technology hub in East Africa – but organized crime accompanies development, and increases avenues for crimes like sex trafficking. Online sexual exploitation is prevalent, mainly targeting women and children on social media apps such as WhatsApp and Telegram.

In Kenya you can find over 50 posts daily 'advertising' victims - over and under 18 - along with a number to call. Rate cards and information about the victim's location, physical appearance and age are given. After, pictures are sent so perpetrators can select who they want and for what services. All arrangements and payments are made through a pimp.

In 2019, a big party organized on social media led to a number of young girls going missing. The families of the missing girls spoke up after videos exposing their sexual abuse surfaced.

The Department of Criminal Intelligence and their officers at police stations are responsible for investigations. But due to lack of training and equipment, officers often do not have the capacity to pull together evidence for online cases.

One of the most difficult things is dealing with police - ask any Kenyan! Reporting a crime is extremely time-consuming and bureaucratic. Some people also shy away from reporting because of victim blaming – the police can ridicule you and have the case turned against you.

For many communities, particularly in rural areas, it is difficult to talk about sexual abuse because it is accompanied by cultural and family shame – rather than focusing on the crime.

Kenya's Trafficking Act and the 2006 Sexual Offences Act provide adequate protections with heavy penalties. The Trafficking Act reflects most international legislation and is in line with the 2000 Palermo Protocol.

But when it comes to implementation it is hard to measure successes, and submissions of evidence to the judiciary, prosecutions, and sentencing remain a challenge. In cases I have followed involving the trafficking of Kenyans to the Middle East, none have reached the prosecution stage even though this is the most prevalent form of trafficking.

There are also issues of detection. Children who have been trafficked are harder to recognize than adults; their trafficker or perpetrator could look like a parent. What's more, some victims are recruited with consent from their families, so we need more monitoring of caregivers, including parents.

During the COVID-19 pandemic, more children have been at home and online, with parents often working. This has led to a rise in sex trafficking and exploitation of children online and needs better monitoring.

The use of technology such as webcams has made it easier to target children. Traffickers craft ways to engage with minors, contacting children and telling them to produce videos. It often starts off with something innocent – a child being told to send photos or videos of themselves dancing – and later they will be told to take off their clothes and send images.

Government schools have also focused on getting students online with digital learning, but I haven't come across any advocacy about internet safety.

"During the COVID-19 pandemic, more children have been at home and online, with parents often working. This has led to a rise in sex trafficking and exploitation of children online, and needs better monitoring."

REGULATION OF DIGITAL SERVICE PROVIDERS AND PLATFORMS

OSEA occurs on online platforms and websites owned and controlled by technology companies. Offenders use digital services and platforms to:

- Identify victims.
- Groom and entrap them.
- Create and share OSEA material.
- Carry out other abuse and exploitation.
- Make and/or receive payments.

Whether digital service providers and platforms should be liable for illegal or harmful content on their platforms or have a legal responsibility to identify, block, or remove this content is highly debated. Generally, service providers and platforms have been considered conduits of information and users' expression of free speech, not publishers of the content, therefore exempting them from liability.[293] This principle is viewed as essential for a well-functioning internet where users can exercise freedom of expression. In almost all of the focus countries, the law provides service providers and platforms with immunity in relation to hosting illegal and/or harmful content on the grounds that either the platforms and providers did not knowingly host the content or they removed it within a certain period of time.

In the US, digital service providers and platforms that comply with best practices can generally claim protection under Section 230 of the CDA should they face civil or criminal lawsuits for third-party content.[294] Likewise, the Indian IT Act[295] provides safe harbor protection to service providers and platforms for user-generated content as long as the service provider or platform observes due diligence.[296] At the time of writing, the UK government had announced the publication of the Online Safety Bill which seeks to establish a new regulatory regime. It would impose duties of care on providers of internet services regarding illegal content and content that is harmful to children and adults.[297]

In Kenya, the Copyright Amendment Act requires service providers and platforms to disable access to the illegal material within 48 hours.[298] The Nigerian Communications Commission (NCC) may also require a corporate entity to remedy its non-compliance with the NCC Internet Code within 14 days.[299] In India, service providers and platforms must observe due diligence and comply with the Intermediaries Guidelines Rules 2011[300] by disabling access to offensive material within 36 hours of learning about it.[301]

293 Some jurisdictions apply a strict liability approach.
294 Section 230(c)(1) of the CDA (US)
295 Section 79(1) of the IT Act (India)
296 Section 79(2)(a), the IT Act (India).
297 Online Safety Bill, 2021. (UK) https://www.gov.uk/government/publications/draft-online-safety-bill
298 See Section 35 of the Copyright Act.(Kenya)
299 Section 9.1 (a) (II) of the Communications Commission Internet Practice Code. (Nigeria) https://www.ncc.gov.ng/docman-main/internet-governance/878-internet-code-practice/file.
300 Section 79(2)(c), the IT Act.
301 Indian IT Act, Intermediary Rules, Rule 3(4)

Ruchira Gupta
Expert Interview

Founder-President
Apne Aap Women Worldwide and
Apne Aap International - India

When the pandemic started in India, there were major social and economic changes with schools closing and lessons going online. Children stopped going into school and an important area of safeguarding was lost. Child protection systems broke down, people lost their livelihoods, and food shelters ran out of food. Poverty is widespread and worsening, and the number of children who are vulnerable to sexual exploitation and abuse has increased.

Tight COVID lockdown restrictions closed off many outlets for young people. Teenagers go through massive changes and their sexuality is burgeoning. Normally, they'd have had their peer group at school to share these feelings and experiences with. But with schools closed, children became isolated at home.

Young people have gone online to build friendships. Predators including traffickers have capitalized on the psychology and vulnerability of victims. Grooming can start with an invitation to talk or play a game, and offenders find ways to seduce and trick children. Boys are also being groomed online to become sex buyers and consumers of pornography.

There are 200 million children in India, and many live below the poverty line. In the country's red light districts, thousands of women and children have faced starvation since the government imposed strict quarantines and mothers were not able to earn money.

Sex traffickers have taken advantage by paying for children in red light districts to be sexually abused online. India is the third largest consumer of pornography and there is big demand for this content. It has also become a leading producer of pornography featuring child sexual abuse, and there is a lot of money being made.

Since the start of the pandemic, ChildLine in India has experienced a 50% rise in calls for help. Some children are stuck at home with their abuser. In these situations, it is common for the family to try to cover things up. We know that children are told to shut up. There are also situations in which family members are scared to report.

Victim blaming is also a problem. If it comes out publicly that a girl has been abused, she faces stigma. People in the community will say she must be sexually active or has done something to cause it.

Victims are being sexually abused and then living with fear and shame. The trauma is something they deal with all their lives, and it can crush them. They lose self-confidence, and they suffer from PTSD, self-blame, anger, and guilt. Without support and counselling, there is a risk that patterns of self-destructive behavior will continue.

A lot can be done to raise awareness, and it's sad that it's not happening. India's government is ignoring the problem. They have a cybercrime cell, but it's not that big and has been used for surveillance, so people are scared of it.

Tech companies can play a bigger role and be huge partners. They should take more responsibility because they're the ones who provide the platforms for this content to flow and they're making lots of money. They say give us data so we can create Artificial Intelligence filters, but this comes up against concerns about digital privacy and the debate is ongoing.

Many adults don't know how to discuss sexual abuse with their kids or how to talk with policy makers. We have to give parents and teachers the tools and opportunities to bring things into the open.

Importantly, we need to have conversations with children so they know they shouldn't carry the burden of responsibility. We need to name abusers and punish perpetrators. It is only by shining a spotlight that we can dispel the dark.

"Children are being sexually abused and then living with fear and shame. They lose self-confidence, and they suffer from PTSD, self-blame, anger, and guilt. Without support and counselling, there is a risk that patterns of self-destructive behavior will continue. [Tech companies] should take more responsibility because they're the ones who provide the platforms for this content to flow and they're making lots of money."

Voluntary Measures to Address Harmful Content

The involvement of technology companies in setting frameworks for practices on their platforms has been supported by some governmental bodies. For instance, the European Commission's Communication on Online Platforms and the Digital Single Market Opportunities and Challenges[302] places considerable responsibility on service providers and platforms to self-regulate in a transparent and effective manner. The Commission suggested it would "explore the need for guidance on the liability of online platforms when putting in place voluntary, good-faith measures to fight illegal content online", and "regularly review the effectiveness and comprehensiveness of voluntary efforts".[303]

The most common form of self-regulation is the platforms' Terms of Use Agreements, Privacy Notices, and Codes of Conduct which dictate acceptable conduct and content, and specify how content that does not meet these standards may be removed.

There has also been a movement towards sector-wide voluntary codes which include guiding principles on how the sector can help address online sexual harms. The codes and principles have tended to focus on children. Notable ones include:

- **The Voluntary Principles to Counter Online Child Sexual Exploitation,**[304] which were issued by the governments of Australia, Canada, New Zealand, the UK, and the US in 2020. The principles were developed in consultation with several leading digital service providers and platforms, including Facebook, Google, Microsoft, Roblox, Snapchat, and Twitter. These companies have endorsed the principles. The 11 principles outline measures that service providers and platforms can implement to protect children from sexual abuse online.
- **The Safer Networking Principles for the EU,**[305] published in 2009, provide guidance on how to manage risks to children online. The principles call on service providers and platforms to "provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service"[306] and "respond to notifications of illegal content or conduct".[307] They should also "assess the means for reviewing illegal or prohibited content/conduct" by making use of measures such as "human and/or automated forms of moderation".[308]
- **Technology coalitions** are another mechanism that has been used to address online sexual abuse of children. For example, Google, Facebook, Twitter, Amazon, Adobe, Apple, PayPal, Snapchat, Roblox, and Microsoft are members of the Technology Coalition,[309] which partners with UNICEF and children's rights organizations, and provides funding and advice to service providers and platforms on implementing child safety tools.[310]
- **Technology tools** developed and used by technology companies to identify and remove OSEA material. Facebook, WhatsApp, and Instagram are making use of tools such as Microsoft's PhotoDNA, Facebook's PDQ, and TMK+PDQF to "crawl" through their platforms to identify and remove CSAM. Technology companies are responsible for the majority of online child sexual exploitation and abuse reports made to NCMEC.[311]

Challenges with Voluntary Measures to Address OSEA

Voluntary codes and initiatives present the following challenges:

- **Difficulties faced by OSEA victims in getting content removed.** Not all service providers and platforms have easy-to-access takedown notice procedures or contact details for victims to send takedown requests. Moreover, in the absence of a criminal investigation, victims may not be able to access information about the perpetrators due to freedom of expression and privacy rights considerations.
- **A lack of precise rules.** Most self-regulatory codes set general targets, which are more statements of intent than clear rules. It is unlikely that private companies would voluntarily commit themselves to ambitious targets.
- **A lack of independent oversight.** Most voluntary codes lack any mechanisms for independent monitoring and oversight. This gap means they may be seen more as public relations exercises than genuine attempts to improve conditions.
- **Weak enforcement and lack of sanctions.** Voluntary codes often do not provide for sanctions for companies in breach. Where they do, they are frequently not enforced. There are concerns as to whether self-regulation can provide robust protection (serving a public interest) and allow service providers and platforms to conduct business efficiently (serving their private interests). Where tensions exist between public interest and private interest, self-

302 Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe 2016 (EU). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0288&from=EN
303 Paragraph 5 of the Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe
304 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/870623/11_Voluntary_principles_-_formal_letter__1_.pdf
305 Safer Networking Principles for the EU, 2009. (EU). The principles were published following consultations between the European Commission and various digital service providers and platforms.
306 Ibid. Note 300 at Principle 4
307 Ibid. Note 300 at Principle 5
308 Ibid. Note 300 at Principle 5
309 https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/
310 For example, on 10 June 2020, the Technology Coalition announced the launch of "Project Protect: A plan to combat online child sexual abuse". As part of Project Protect, the Technology Coalition has committed to invest in innovative tech to tackle CSAM on the web. https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/
311 See https://www.iicsa.org.uk/key-documents/17805/view/internet-investigation-report-march-2020.pdf

regulation is ineffective and governments need to play a more active role.

- **Failure of automated tools to detect and remove all types of OSEA material.** Although automated tools enable large amounts of illegal and harmful content to be removed and for law enforcement to access information for prosecutions, the tools tend to focus on CSAM. More is required in identifying and removing abusive material depicting other vulnerable groups like women. Automated tools do not always identify material depicting adolescent girls, who may have similar physical features to adult females. This is a significant challenge because laws on illegal and harmful content tend to focus on children. The tools have also had difficulties in identifying altered images and deepfakes. Companies like Facebook are investing large sums of money to improve the ability to identify and remove altered images in response to the growing problem.[312]

Calls for Tougher Regulation

In light of the challenges presented by voluntary measures, a growing call has emerged to make service providers and platforms responsible and liable through legally binding rules. Among the focus countries, there is some movement, albeit slow, towards making the companies accountable in law.

International Level

Although not legally binding, a number of calls at the international level have demanded greater accountability be placed on digital service providers and platforms. The UN Guiding Principles on Business and Human Rights state that businesses have a responsibility to respect human rights.[313] The Principles also assert that businesses should take steps to enable effective remediation of any adverse human rights impact they cause or contribute to.[314]

Regarding the protection of children, the CRC Guidelines recommend that States ensure that digital service providers and platforms control, block, and remove CSAM as soon as possible.[315] The CRC Guidelines also recommend that States require by law that ICT companies block and remove CSAM on their servers and financial institutions block and refuse financial transactions intended to pay for such offenses.[316]

Recently, CEDAW's Recommendation 38 called on States to ensure that digital service providers and platforms take responsibility "for exposure of women and girls to trafficking and sexual exploitation as users of their services"[317] and required them to define controls to mitigate technology-facilitated trafficking of women and girls.

European Level

The EU Directorate-General for Internal Policies[318] has called for the creation of a single EU-level Code of Conduct for social media platforms providing services used by children, "underpinned by strong backstop powers," to conduct independent monitoring. It recommends there be a trusted and sufficiently resourced body to ensure compliance with the Code, and with significant sanctions at its disposal. The EU is also considering a Digital Services Act that would require service providers and platforms to remove illegal content or face sanctions.[319]

Laws in the UK and US

The UK and the US have been at the forefront in calling for laws to enhance safety online. In the US, ongoing debates continue about reforming the CDA as well as enactment of other laws that would protect vulnerable groups like children and hold technology companies accountable.

In the UK, the recently published Online Safety Bill seeks to impose duties of care on providers of digital service providers and platforms to make them responsible for content generated and shared by their users and to mitigate the risk of harm arising from illegal content. The Bill also designates the Office of Communications (OFCOM) to oversee and enforce the new regime and requires OFCOM to prepare codes of practice to outline recommendations for businesses to comply with their duties.

Arguments Against Tougher Regulation

While tougher regulation is seen as part of the solution to address OSEA, some have raised concerns regarding its impact on freedom of expression and technology innovation, such as:

- **Removing tech immunity will "stifle freedom of expression."** Some campaigners argue that laws such as FOSTA-SESTA, which create exceptions to Section 230 immunity, are at odds with freedom of expression as they force internet platforms to censor users. These proponents claim Section 230 of the CDA already strikes a careful balance between enabling the pursuit of justice and promoting free speech: platforms can be held responsible for their own actions and can still host user-generated content without fear of broad legal liability. They argue that without Section 230 of the CDA, the internet would not function in the way it does now, and many of today's platforms would never have existed because the risk of litigation would be too high.
- **Concerns that regulation may impede innovation.** There are concerns that stricter rules would impede and discourage business opportunities and innovation. These

312 See https://www.bbc.com/news/technology-51018758
313 Op. cit. Note 286 at Principle 11
314 Op. cit. Note 286 Principle 15
315 Op. cit. Note 55 at Paragraph 41
316 Op. cit. Note 55 at Paragraph 79
317 Paragraph 71 of CEDAW General Recommendation (38) on trafficking in women and girls in the context of global migration.
318 http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/617454/IPOL_IDA%282018%29617454_EN.pdf
319 European Commission. The Digital Services Act package. https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

rules would particularly impact smaller companies and start-ups that would not be able to comply with the strict rules or afford litigation costs.

Conclusion

Voluntary regulation and the current frameworks for holding digital service providers and platforms liable for user-generated content is clearly not working. A new regulatory framework is required to provide clarity and guidance on the expected behavior of digital technology companies, the extent of their accountability, and their liability with regard to illegal and harmful user-generated content. A new regulatory framework is also required to protect vulnerable people and combat the evolving nature of online abuse while also balancing the concerns of privacy, freedom of expression, and innovation.

The role of the technology sector in addressing OSEA cannot be underestimated. It is with their technology and on their platforms that perpetrators sexually exploit and abuse vulnerable people. Within a regulated framework, companies' technology can play a bigger role in detecting and removing OSEA material and preventing users from creating and sharing it.

The input of governments, technology companies, human rights organizations, civil society actors, and survivors of OSEA is needed to strike the right balance when drawing up a stronger regulatory framework.


REUTERS/Harun Ucar

CONCLUDING REMARKS

The analysis in this report affirms that OSEA is a global, gendered, and multi-dimensional problem that requires coordinated responses from the international community. National efforts, including laws, have to be supported by strong interconnected international efforts. The global response is critical to ensure adequate protection for all people everywhere.

At all levels, the law has not kept up with the evolving nature of technology and OSEA. Instead, there is a patchwork of legislation with different, but not all, aspects of OSEA addressed across international and regional laws and standards. In addition, there is limited attention paid to the gendered dimensions of OSEA, which has resulted in groups like women and adolescent girls not being adequately protected.

Where they do not exist, laws that address online misogyny and gender and intersecting inequalities need to be enacted and enforced to target the root causes of OSEA. International human rights laws provide frameworks like the proportionality test that can be used to balance between protection and freedom of expression and privacy. There is an opportunity for States to use these mechanisms in the context of OSEA. First, however, there must be laws to protect against OSEA in all of its forms. Laws must also hold digital service providers and platforms accountable for OSEA.

RECOMMENDATIONS

INTERNATIONAL COMMUNITY (NATIONAL GOVERNMENTS AND REGIONAL AND INTERNATIONAL BODIES)

Develop and Adopt Binding International Standards

The international community should develop and adopt legally binding international standards that provide for protection of all vulnerable people from all forms of OSEA. The international standards would demonstrate consensus on the severity of OSEA and provide a framework for legal implementation, policies, programs, and international cooperation.

The international legal standards should:

- Provide a standard definition of OSEA, and its various forms, including its consumption and distribution. The definition should be future-proofed to ensure that it takes into account the evolving nature of OSEA.
- Take into account the gendered nature of OSEA, recognizing it as part of the continuum of gender-based violence and highlighting the particular vulnerabilities and needs of women and girls and other vulnerable people.
- Provide a framework on international cooperation to address the multi-jurisdictional nature of OSEA, and provide guidance in areas such as prosecutions and investigations.
- Provide for national obligations in the identification, support, compensation, and non-punishment of OSEA victims.
- Clarify the role, responsibility, and accountability of digital service providers and platforms, in preventing, detecting, and reporting OSEA on their platforms.
- Provide for the regulation of user-generated content, and moderation of online content by service providers and platforms.
- Include guidance on reporting mechanisms on digital platforms (for example, takedown notices) for aggrieved persons, limitation of liability for digital platforms, cross-jurisdictional collaboration, and reporting mechanisms.
- Clarify the balance between protection and safety from exploitation and abuse and the rights of freedom of expression and privacy online.

Review and Update Existing International and Regional Instruments

In the medium term, international and regional instruments, particularly those relating to women's rights, children's rights, violence against women and girls, cyber-crime, and those dealing with rights such as privacy and freedom of expression, should be reviewed and updated to ensure they are aligned to the reality of the digital age and prospective international standards.

In the case of binding legal instruments, updating can be achieved through General Comments and Recommendations of human rights treaty monitoring bodies that would:

- Explain the extent to which existing legal instruments serve to protect vulnerable people and address OSEA. For instance, other treaty bodies can follow the example of the CRC Committee which has adopted a General Recommendation on the Rights of Children in the Digital Age.
- Provide for national obligations in the identification and support of OSEA victims.
- Clarify the role, responsibility, and accountability of digital service providers and platforms, in preventing, detecting, and reporting OSEA on their platforms.
- Provide recommendations to national governments on prevention, prosecution, legal and policy adoption and implementation, and international cooperation to address OSEA.

Conduct Up-to-Date Research and Analysis on OSEA

International and regional organizations can work with governments to conduct research on OSEA to enable countries to have up-to-date information to respond to emerging trends and issues.

The research and analysis should:

- Provide up-to-date information on regional, national, and international trends on OSEA.
- Identify new forms of OSEA and survivor experiences, including new ways perpetrators are taking advantage of evolving technology.
- Take into account and provide up-to-date information and analysis on the gendered nature and implications of OSEA and the impact on women and girls.
- Provide ongoing examples of good legal practices, policies, and actions of stakeholders that can be adapted in different jurisdictions, including ways law enforcement can respond to the implications of evolving technology.

GOVERNMENTS

Review and Update Legislation and Policies to Fully Protect Vulnerable People from OSEA

Governments must ensure that domestic laws and policies on OSEA align with international standards, where they exist, including providing for protection of vulnerable people. Domestic laws should also take into account the gendered, technological, and multi-jurisdictional nature and dimensions of OSEA. Domestic laws and policies can play an important role in changing attitudes and behaviors.

Governments should:

- Enact and implement laws that address the root causes of OSEA, in particular gender, sex-based discriminations and intersecting inequalities and the proliferation of misogyny and abuse of power online.
- Provide legislative measures enabling law enforcement to investigate and prosecute perpetrators of OSEA across jurisdictions.
- Implement laws facilitating identification and provision of support services, and compensation and non-punishment of OSEA survivors.
- Cooperate to ensure that when OSEA material is shared, posted, or otherwise published outside a country's jurisdiction (including on websites registered elsewhere) it is removed and blocked from further sharing as soon as possible, and those who shared, posted or otherwise published such materials are appropriately penalized.
- Mandate that digital service providers and platforms have easy-to-use takedown notice procedures. These procedures should enable victims, their representatives, and families to provide the service providers and platforms with information that is adequate to identify the material or a portion thereof.
- Mandate that service providers and platforms respond to takedown requests within a reasonable time.
- Mandate that digital service providers remove and block all OSEA materials from further sharing or publication and destroy all OSEA materials as soon as they are discovered; provided such destruction does not serve to remove evidence necessary to investigate and prove the crime.
- Mandate penalties, including fines, when digital service providers and platforms fail to comply with the law, including additional penalties for continued breaches and failure to comply.
- Establish an independent regulatory authority to oversee the implementation of laws and regulations.

Strengthen National Capacity to Address OSEA

In addition to strong laws, we encourage governments to strengthen national institutions through provision of adequate resources to investigate and prosecute OSEA cases, and support victims' access to the legal system.

Governments should:

- Provide adequate funding to key institutions including law enforcement, the judiciary, child protection services, and women's rights departments, towards investigating and prosecution of cases, and support to victims and survivors of OSEA.
- Ensure law enforcement has access to the technology and equipment required to conduct proper investigations.
- Increase knowledge, through training and other measures, of key institutions including law enforcement, human rights institutions, the judiciary, child protection services, and women's rights departments on OSEA and their responsibility to addressing it.
- Conduct awareness raising campaigns for citizens to become more aware of their rights online and how to report violations of those rights.

Collaborate with Other Key Stakeholders

Ending OSEA requires collaboration amongst countries, civil society organizations, digital technology companies, survivors, and survivor-led organizations.

Governments should forge collaborations by:

- Working with civil society and the media to raise understanding of OSEA including information on how to identify and report to law enforcement and digital service providers and platforms.
- Working with civil society organizations and survivors to identify the interventions necessary to address OSEA that take into account experiences and perspectives of survivors.
- Engaging digital service providers and platforms and the private sector at large in the development and use of technological tools to prevent, detect, and remove OSEA material.
- Engaging digital service providers and platforms and the private sector at large to collaborate on information sharing to enable and support investigations of OSEA.
- Ensuring and facilitating collaboration among national law enforcement and regional and international agencies such as INTERPOL to enhance skills and capacity to investigate OSEA nationally and across jurisdictions.

DIGITAL SERVICE PROVIDERS AND PLATFORMS

Apply Human Rights Approach and Standards in Policies and Practices

Digital service providers and platforms should adopt a human rights-based approach in their policies, including terms of use and community standards. A human rights-based approach should also be applied in content moderation policies.

Digital service providers and platforms should:

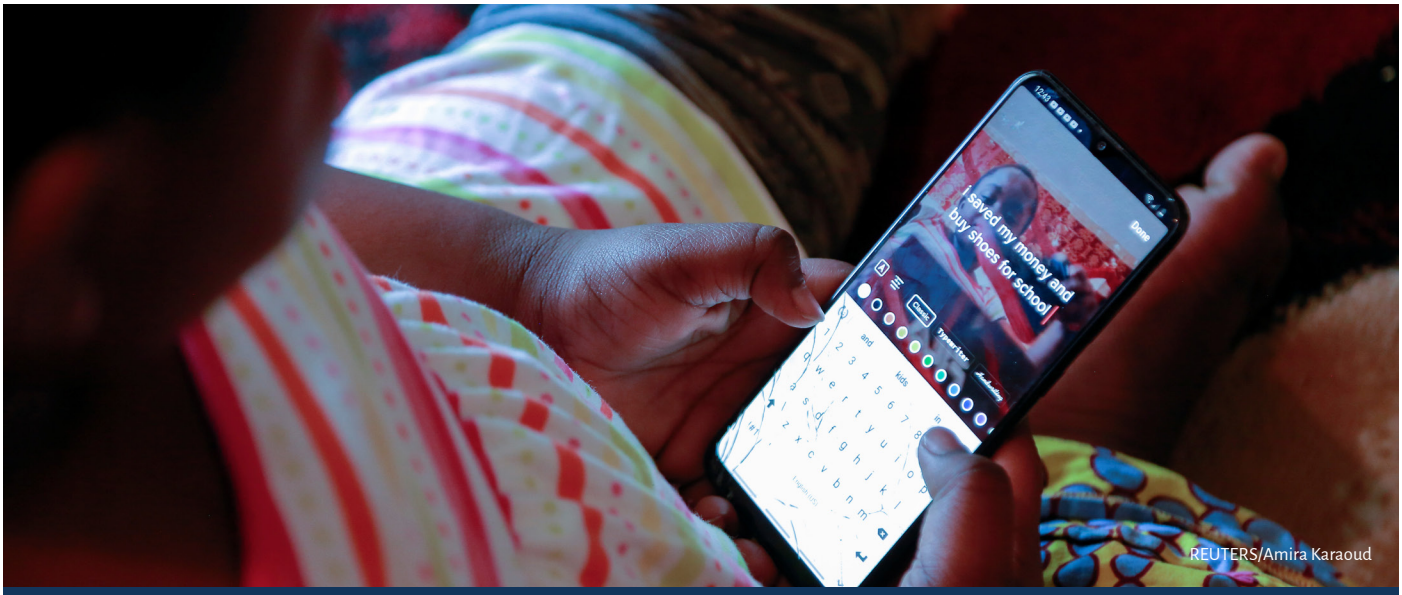
- Adopt policies and practices reflecting the user's right to protection from harm and the right to dignity and privacy. The practices should include ensuring harmful content is identified and removed before it is posted on their platforms.
- Adopt policies and practices that acknowledge a responsibility to protect users.
- Educate users on their rights and empower users to seek recourse when those rights have been violated.
- Implement takedown notice procedures that are easy to use and find.
- Be transparent and accountable in policies and practices regarding the moderation of OSEA and the extent to which policies and practices have been effective.

Collaborate with Governments and Other Stakeholders

Digital service providers and platforms, governments, and other stakeholders should collaborate to address OSEA.

Digital service providers and platforms should:

- Continue to share technological knowledge and expertise with law enforcement agencies to support the investigation of OSEA.
- Develop, deploy, and promote technological tools to prevent, detect, and remove all OSEA material.
- Widen the scope of tools used to find and remove OSEA to include identifying content with adolescent girls and women.
- Engage with organizations working with survivors and perpetrators to share knowledge on exploitation pathways, survivor experiences, and input on solutions.
- Raise awareness among CSOs and law enforcement on their reporting tools and mechanisms on their platforms.
- Work with governments to develop technological solutions to address the upholding and generation of OSEA content on their platforms.



REUTERS/Amira Karaoud

ANNEXES

ANNEX 1 - INTERNATIONAL LEGISLATIVE MAPPING

- Convention Against Transnational Organized Crime
- Convention against Corruption
- Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (Worst Forms of Child Labour Convention)
- Convention on the Elimination of All Forms of Discrimination Against Women
- Convention on the Rights of the Child
- Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)
- International Covenant on Civil and Political Rights
- Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (CRC Optional Protocol)
- Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (Palermo Protocol)
- Universal Declaration of Human Rights

International Legislative Status

	India	Kenya	Nigeria	U.S.	U.K.
CEDAW	RATIFIED	RATIFIED	RATIFIED	SIGNED	RATIFIED
CRC	RATIFIED	RATIFIED	RATIFIED	SIGNED	RATIFIED
CRC Optional Protocol	RATIFIED	SIGNED	RATIFIED	RATIFIED	RATIFIED
ICCPR	RATIFIED	ACCEDED	RATIFIED	RATIFIED	RATIFIED
Palermo Protocol	RATIFIED	ACCEDED	RATIFIED	RATIFIED	RATIFIED
Worst Forms of Child Labour Convention	RATIFIED	RATIFIED	RATIFIED	RATIFIED	RATIFIED

The Table shows the ratification status of some of the relevant international legislation.

ANNEX 2 - RELEVANT NON-BINDING INTERNATIONAL INSTRUMENTS MAPPING

- Beijing Declaration and Platform for Action
- Declaration on the Elimination of Violence against Women
- Vienna Declaration and Programme of Action
- Guiding Principles on Business and Human Rights
- Sexual And Gender-Based Violence Against Refugees, Returnees And Internally Displaced Persons: Guidelines For Prevention And Response (UNHCR Guidelines)
- The Yokohama Global Commitment
- UN High Commissioner for Refugees (UNHCR). Sexual and Gender-Based Violence against Refugees, Returnees and Internally Displaced Persons. Guidelines for Prevention and Response

ANNEX 3 - REGIONAL LEGISLATIVE MAPPING

Africa

- African Charter on Human and Peoples' Rights
- Convention on Cybersecurity and Personal Data Protection (Malabo Convention)
- Declaration of Principles of Expression and Access to Information in Africa
- Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol)
- Supplementary Act A/SA.1/01/10 on Personal Data Protection

Americas

- Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women (Belém do Pará Convention)
- American Convention on Human Rights

Europe

- Convention for the Protection of Individuals with regard to the Processing of Personal Data, No. 108+
- European Convention on Human rights
- The EU Anti-trafficking Directive 2011/36/EU
- Combating Sexual Abuse of Children Directive 2011/93/EU
- Directive 2012/29/EU of the European Parliament and the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA
- EU Guidelines on Freedom of Expression Online and Offline

ANNEX 4 - THE FIVE FOCUS COUNTRIES LEGISLATIVE MAPPING

India

- Code of Criminal Procedure, 1973
- Constitution of India, 1949
- Penal Code, 1860
- Indecent Representation of Women (Prohibition) Act, 1986
- Information Technology Act, 2000
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Protection of Children from Sexual Offences Act, 2012

Kenya

- Children Act, 2010
- Computer Misuse and Cybercrimes Act, 2018
- Copyright Act, 2001
- Counter Trafficking in Persons Act, 2010
- Data Protection Act, 2019
- Employment Act, 2007
- Extradition (Commonwealth Countries) Act, 1968
- Mutual Legal Assistance Act, 2011
- Penal Code, 2018
- Sexual Offences Act, 2006

Nigeria

- Criminal Code Act, 2004
- Cybercrimes (Prohibition, Prevention, etc.) Act, 2015
- Data Protection Regulation, 2020
- Mutual Assistance in Criminal Matters Act, 2019
- Trafficking in Persons (Prohibition) Enforcement and Administration Act, 2015

UK

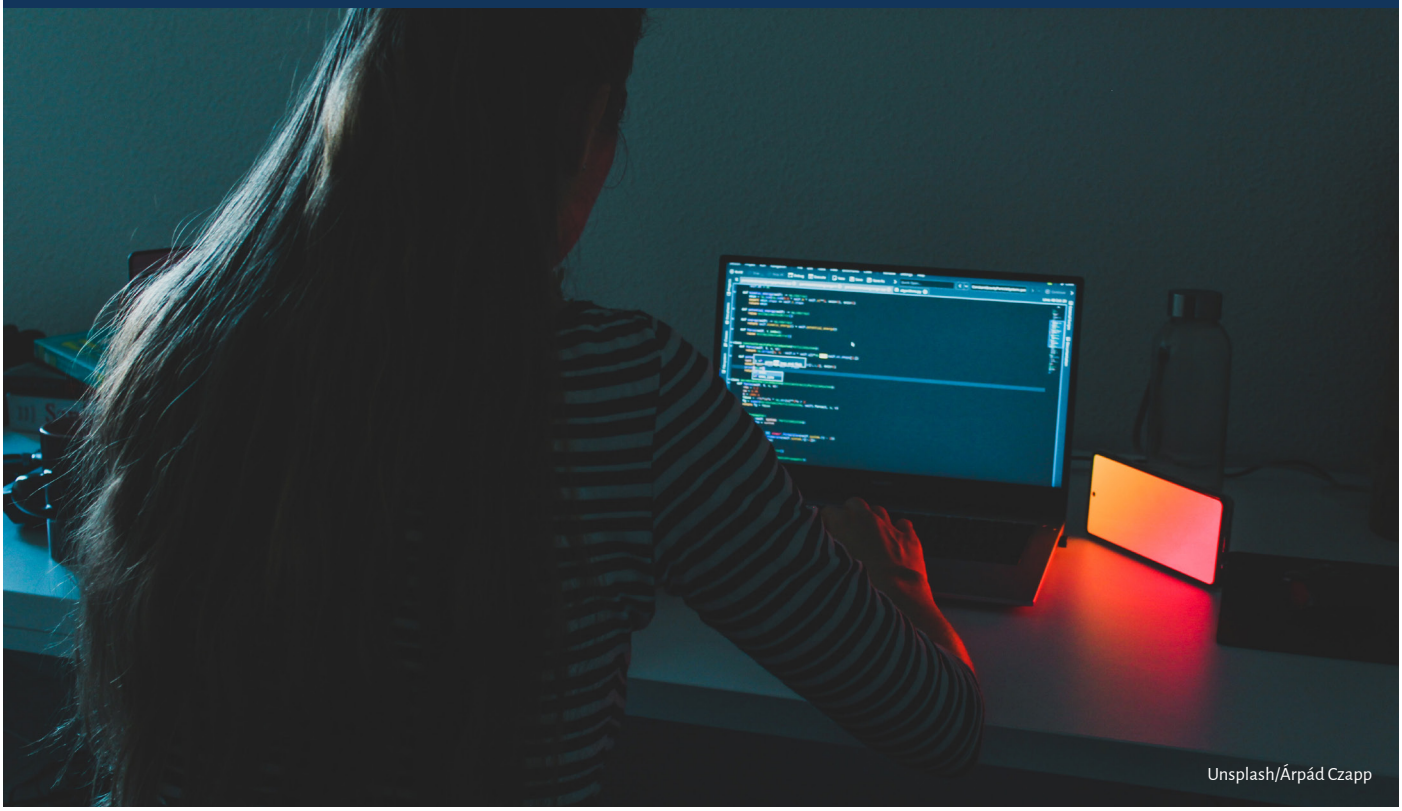
- Criminal Justice and Immigration Act, 2008
- Criminal Justice and Courts Act, 2015
- Communications Act, 2003
- Extradition Act, 2003
- Malicious Communications Act 1988
- Modern Slavery Act, 2015
- Protection of Children Act, 1978
- Protection from Harassment Act, 1997
- Sexual Offences Act, 2003
- Serious Crimes Act, 2015

US

- Child Pornography Prevention Act, 1996
- Children's Online Privacy Protection Act, 1998
- Clarifying Lawful Overseas Use of Data Act, 2018
- Communications Act, 1934
- Constitution of the United States, 1788
- The Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act, 2017
- Florida Statute 800.04(5)
- New Jersey statute section NJSA 2C:14-9
- Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act, 2003
- Stored Communications Act, 1986

OSEA Resources and Support Information

- https://cccr-nigeria.org
- https://www.cybervictims.org
- https://endtab.org
- https://report.cybertip.org
- https://www.tracekenya.org
- https://www.rainn.org/national-resources-sexual-assault-survivors-and-their-loved-ones
- https://voic.org.uk



Unsplash/Árpád Czapp