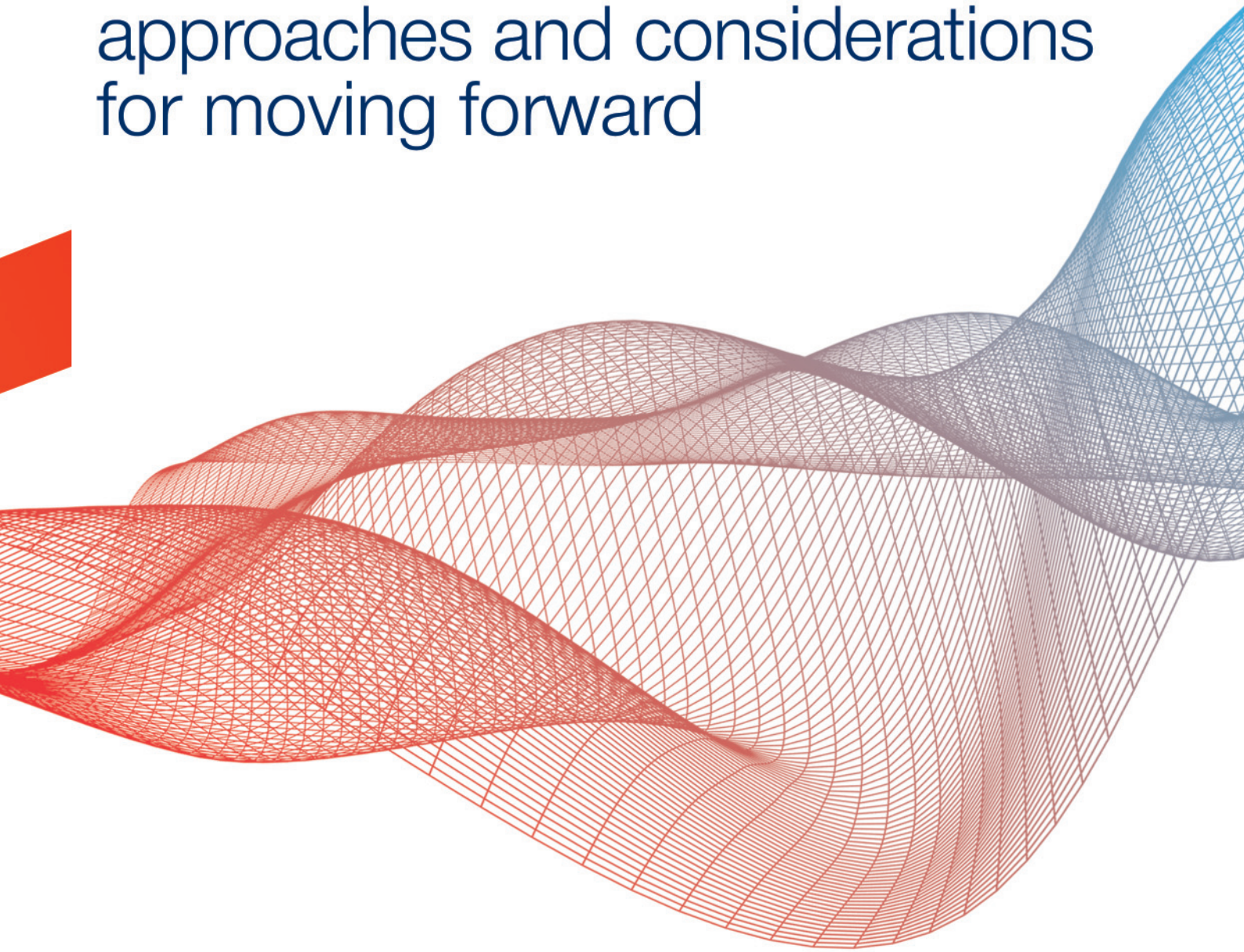
Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings

Policy responses to technology-facilitated trafficking in human beings:

Analysis of current approaches and considerations for moving forward



OSCE Organization for Security and Co-operation in Europe

ISBN: 978-3-903128-80-4

Published by the OSCE Office of the Special Representative
and Co-ordinator for Combating Trafficking in Human Beings

Wallnerstrasse 6, 1010 Vienna, Austria
Tel: + 43 1 51436 6664
Fax: + 43 1 51436 6299
email: info-cthb@osce.org

Design: Vitalie Ciupac

Cite as: OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Policy Responses to Technology-Facilitated Trafficking in Human Beings: Analysis of Current Approaches and Considerations for Moving Forward (Vienna, March 2022)

The Organization for Security and Co-operation in Europe (OSCE) is a pan-European security body whose 57 participating States span the geographical area from Vancouver to Vladivostok. Recognized as a regional arrangement under Chapter VIII of the United Nations Charter, the OSCE is a primary instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation in its area. Its approach to security is unique in being both comprehensive and co-operative: comprehensive in that it deals with three dimensions of security – the human, the politico-military and the economic/ environmental. It therefore addresses a wide range of security-related concerns, including human rights, arms control, confidence- and security-building measures, national minorities, democratization, policing strategies, counter-terrorism and economic and environmental activities.

PARTICIPATING STATES: Albania | Andorra | Armenia | Austria | Azerbaijan | Belarus | Belgium | Bosnia and Herzegovina | Bulgaria | Canada | Croatia | Cyprus | Czech Republic | Denmark | Estonia | Finland | France | Georgia | Germany | Greece | Holy See | Hungary | Iceland | Ireland | Italy | Kazakhstan | Kyrgyzstan | Latvia | Liechtenstein | Lithuania | Luxembourg | Malta | Moldova | Monaco | Mongolia | Montenegro | Netherlands | North Macedonia | Norway | Poland | Portugal | Romania | Russian Federation | San Marino | Serbia | Slovakia | Slovenia | Spain Sweden | Switzerland | Tajikistan | Turkey | Turkmenistan | Ukraine | United Kingdom | United States of America | Uzbekistan

ASIAN PARTNERS FOR CO-OPERATION: Afghanistan | Australia | Japan | Republic of Korea | Thailand
MEDITERRANEAN PARTNERS FOR CO-OPERATION: Algeria | Egypt | Israel | Jordan | Morocco | Tunisia

Table of contents

Preface


OSCE/Ghada Hazim

Technology is one of the most important topics in the anti-trafficking field today. The use and misuse of technology permeates virtually every aspect of the crime and its response. For these reasons, addressing the role of technology vis-à-vis the crime of trafficking in human beings (THB) has been a priority of my Office for a number of years. This work began by recognizing the positive role that technology can play in combating THB, mapping the technology tools used by anti-trafficking practitioners in the OSCE region and beyond, and raising awareness about the potential of such tools to help identify victims and investigate cases of THB.[1]

We have also examined the myriad ways that technology is misused by traffickers across all aspects of the THB business model, including recruitment, control and exploitation. Our research revealed that inadequate attention has been given to understanding how States are addressing technology-facilitated THB from a policy perspective. Nor has the rationale or impact of various regulatory models on different technology sectors been sufficiently examined. The publication before you is an attempt to close this gap and bring more clarity to the topic.

This report provides an analysis of how technology-facilitated THB has been approached from the perspective of policy and legislation across the OSCE participating States. While looking primarily at the accelerating shift toward government-led responses, the report also examines the policies and practices adopted by the private sector and civil society organizations. These non-State initiatives are important for many reasons, including the innovative approaches they have taken, as well as their successes and failures which offer insight into how different sectors can be impacted by future policy development at the State level. In addition, the report offers recommendations for policy and legislative responses by OSCE participating States to the misuse of technology to exploit THB victims.

This report does not present model legislation. Its focus is on the most important elements of the policy debate around technology-facilitated THB, such as self-regulation versus government-led regulation, voluntary versus mandatory compliance, and the balance of sector-specific considerations that might lead policy makers to propose appropriate regulations related to: monitoring, reporting, transparency, liability, content removal, and blocking of online platforms. We believe that without understanding these important concepts, the pros and cons of different approaches, and how they influence the technology-facilitated THB landscape, policymakers cannot engage in a meaningful conversation about the laws and policies needed in their countries.

A unique feature of the report is that it focuses on policy aspects related to technology-facilitated THB of both minors and adults. A significant part of the current global anti-trafficking effort is dedicated to children, especially with regard to their online sexual exploitation or the creation and distribution of child sexual abuse material. This emphasis is understandable given the vulnerability of children and the harm they are exposed to. Nonetheless, the problem of exploitation of adults through the misuse of technology

1 See OSCE and Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools* (Vienna: OSCE and TAT, 22 June 2020).

also needs to be urgently addressed, since more and more adult victims of THB for sexual exploitation are being exploited online.

Discussions about policies and legislation related to technology companies and THB can often be sensitive. Arguments have been put forward that private companies should not be regulated, and attempts to do so are often framed as a threat to internet freedom or other rights. At the same time, the persistent nature and scale of harms perpetrated with the assistance of technology demands a new and more robust response that is tailored to the unique risks presented by different technologies (e.g. social media presents challenges, and requires solutions, that can often be different from file storage services which are different from private message boards).

The complexities of technology-facilitated THB require a "whole of society" approach and a set of comprehensive and targeted measures that are up to the task. In light of the clear limitations of the traditional self-regulation approach founded on voluntary action, the time has clearly come for mandatory, State-led policies that bring a harmonized approach to combating technology-facilitated THB.

I hope that this report will serve as a useful resource to support the ongoing dialogue regarding the best ways to address technology-facilitated THB, and that it will assist policymakers, civil society and technology companies to take optimal decisions in their endeavour to end the misuse of technology for THB purposes.

Valiant Richey

OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings

Acknowledgements

This publication has been prepared under the lead of Radu Cucos, Associate Officer in my Office, and peer reviewed by Oleksandr Kyrylenko, Programme Officer, Evan Karr, Assistant Officer, as well as Ignacio Talegon Campoamor, Senior External Co-operation Officer and Arina Nachinova, Intern in the Office of the OSCE Secretary General.

I would like to express my appreciation to the following external consultants who contributed to the drafting of this publication: Livia Wagner, Senior Expert, Global Initiative Against Transnational Organized Crime; Thi Hoang, Analyst and JIED Managing Editor, Global Initiative Against Transnational Organized Crime; and Lucia Bird Ruiz-Benitez de Lugo, Senior Analyst, Global Initiative Against Transnational Organized Crime. I would also like to thank Haley McNamara, Director of the International Centre on Sexual Exploitation and the Vice President of the National Center on Sexual Exploitation for contributing with inputs to the report. Their diligent and professional work contributed greatly to this report.

I would also like to extend our appreciation to Jessica Harrison, Operations Manager at the Modern Slavery and Trafficking Unit of the UK National Crime Agency, Ayelet Dahan, Deputy Anti Trafficking Coordinator, Ministry of Justice of Israel, Alexandra Karra, Senior Attorney, Cybercrime Department, State Attorney's Office, Ministry of Justice of Israel, Anu Leps, National Coordinator against Trafficking in Human Beings, Ministry of Justice of Estonia, representatives of the Ministry of Justice of the Republic of Georgia, representatives of the state institutions of Montenegro and Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation for agreeing to be interviewed in the process of drafting of this publication and for sharing their knowledge and experience on policy aspects related to technology-facilitated human trafficking.

Let me also thank the technology companies, including Apple, Microsoft and Snapchat, for reviewing the content of the publication from the point of view of the technology sector and providing informed feedback.

Finally, my gratitude goes to Cynthia Peck-Kubaczek for her careful editing and proofreading of the text, and to Vitalie Ciupac for designing the publication.

Valiant Richey

OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings

Acronyms and abbreviations

CEDAW	Committee on the Elimination of Discrimination Against Women
CSAM	Child Sexual Abuse Material
CSE	child sexual exploitation
CSEM	child sexual exploitation material
CSEC	commercial sexual exploitation of children
ECJ	European Court of Justice
ECPAT	End Child Prostitution and Trafficking
EU GDPR	General Data Protection Regulation of the European Union
ICT	information and communication technology
ISP	internet service provider
NCMEC	National Center for Missing and Exploited Children
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
THB	trafficking in human beings
UNCRC	United Nations Convention on the Rights of the Child
UNICEF	United Nations International Children's Emergency Fund
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organized Crime
USAID	United States Agency for International Development

Glossary of key terms

Budapest Convention: Council of Europe, Convention on Cybercrime, 23 November 2001.
Instrument serving as a guide for countries developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State parties.[2]

Child sexual abuse material
Material depicting acts of sexual abuse and/or focusing on the genitalia of children.[3]

Cybercrime
Criminal acts committed online using electronic communications networks and information systems.[4]

Cyber security
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.[5]

Digital Services Act (DSA)
A legislative proposal of the European Commission that was submitted to the European Parliament and the European Council on 15 December 2020. The DSA is one of two proposals of the Digital Services Act package. The Act builds on the e-Commerce Directive to address new challenges online.

E-Commerce Directive 2000/31/EC of 8 June 2000
The foundational legal framework for online services in the EU. It aims to remove obstacles to cross-border online services.[6]

Encrypted communication/ Encryption
Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used.[7]

FOSTA-SESTA
Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) and Stop Enabling Sex Traffickers Act (SESTA) are the U.S. Senate and House bills that became law on 11 April 2018 as the FOSTA-SESTA package.

Lanzarote Convention: Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, 25 November 2007.
Instrument that criminalizes a broad range of sexual offences against children. It sets out that parties shall adopt specific legislation and take measures to prevent sexual violence, to protect child victims and to prosecute perpetrators.[8]

Notice and take down
A mechanism whereby an internet intermediary is called upon directly by a private entity (individual, company, rights holders organization, etc.) to remove or disable access to information in response to a breach of their rights (or more generally, of the law). In the EU, a notice and take-down mechanism is implied, but not directly provided, in Article 14 of the E-Commerce Directive 2000/31/EC.[9]

Online Platform
Digital service[s] that facilitate interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet.[10]

Palermo Protocols
Protocols adopted by the United Nations to supplement the UNTOC (UN Convention on Transna-

2 See Council of Europe, *Convention on Cybercrime* (Budapest: Council of Europe, 23 November 2001).

3 See Susanna Greijer and Jaap Doek, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (Luxembourg: ECPAT International, June 2016), p. 40. Available at: www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology (accessed 29 November 2021).

4 See European Commission, *Cybercrime* [website] (European Commission). Available at: www.ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (accessed 21 October 2021).

5 See Computer Security Resource Center, *Glossary – Cyber security* [website] (National Institute of Standards and Technology, U.S. Department of Commerce). Available at: www.csrc.nist.gov/glossary/term/cyber security (accessed 21 October 2021).

6 See European Parliament and European Council, *Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal market (Directive on electronic commerce)* (Official Journal of the European Communities L 178/1, 17 July 2000).

7 See Computer Security Resource Center, *Glossary – encryption* [website] (National Institute of Standards and Technology, U.S. Department of Commerce). Available at: www.csrc.nist.gov/glossary/term/encryption (accessed 21 October 2021).

8 See Council of Europe, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote: Council of Europe, 25 October 2007).

9 See Aleksandra Kuczerawy, "From 'Notice and Take Down' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression", in: Giancarlo Frosio (ed.), *The Oxford Handbook of Intermediary Liability Online* (Oxford: Oxford University Press, 2020), chapter 27.

10 See OECD, *An Introduction to Online Platforms and their Role in the Digital Transformation* (OECD, 13 May 2019), p. 21. See also, European Parliamentary Research Service, *Liability of Online Platforms* (European Parliament, February 2021), p. 12.

tional Organized Crime, also known as the Palermo Convention). They are the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing and Trafficking in Firearms, Their Parts and Components and Ammunition.

Technology-facilitated trafficking in human beings
Refers to trafficking in human beings offences occurring or facilitated through the use of technology.

Safe harbour
An exemption or immunity from liability, sometimes as the result of having taking certain action such as due diligence. For example, the European Union's E-commerce Directive introduces a safe harbour principle under which three types of online intermediaries who host or transmit content provided by a third party are exempt from liability under certain conditions.

Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse[11]
The Voluntary Principles were developed following an action agreed at the Five Countries Ministerial meeting held in London in July 2019. A working group of officials from New Zealand, Australia, the United Kingdom, the United States and Canada worked in consultation with some larger technology companies to develop the principles.

11 See US Department of Justice, "Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse" [website] (the United States Department of Justice). Available at www.justice.gov/opa/press-release/file/1256061/download (accessed 21 October 2021).

Introduction

1. The challenge

It has been almost 35 years since Melvin Kranzberg stated "technology is neither good nor bad – nor is it neutral".[12] Technology has changed significantly since then, and it has proved to be a double-edged sword:[13] in the context of trafficking in human beings (THB), technology is the principal industry sector that has the potential to be both part of the problem and part of the solution in finding effective ways to address human trafficking.

Internet and communication technology (ICT) has led to the emergence and rapid expansion of technology-facilitated THB offences. Indeed, the misuse of technology has become central to the modus operandi of trafficking networks and perpetrators globally. At the most basic level, ICT – and the internet specifically – facilitates connectivity among perpetrators, between traffickers and their victims, as well as with users of goods and services extracted from victims.[14]

However, framing the issue merely in terms of facilitating person-to-person communication vastly understates the impact of ICT on THB. Human trafficking can be understood as an illicit marketplace where people are treated as commodities, a market that is governed by dynamics of supply, demand, price and competition.[15] A key concern is that the misuse of technology is contributing to the overall expansion of the THB marketplace, increasing efficient interaction between illicit supply and demand, as well as fostering ever greater proceeds. While the proceeds of crime are difficult to estimate, research undertaken by the International Labour Organization (ILO) points to a fivefold increase in the profits generated by human trafficking/forced labour in the decade between 2005 and 2014, with profits reaching an estimated US $150 billion per year.[16]

Technology has enabled traffickers to operate more efficiently, while dramatically expanding their reach. This has effectively increased the scale, geographic scope and speed at which THB crimes are being committed.[17] Technology also offers new opportunities for human traffickers, in essence increasing the forms of THB. For example, the livestreaming of sexual acts - predominantly involving children - to a typically closed audience is one relatively new and rapidly expanding technology-facilitated phenomenon that is extremely difficult to curtail.

As technology becomes ever more central to both licit and illicit marketplaces, the challenge posed by technology-facilitated THB is set to increase. Effective responses are urgently required. In particular, attention to fostering safety and countering the harms – including substantive human rights violations – facilitated by the misuse of technology is needed.

2. The response

Responding to the growth of technology-facilitated THB has been recognized by the international community as a key challenge, particularly in the area of capacity building. For example, in Resolution 27/2 of 2018 of the Commission on Crime Prevention and Criminal Justice, UN Member States mandated UNODC to "continue providing, within its existing mandate, technical assistance and training to Member States, in particular developing countries, at their request, to improve and build capacities to prevent and combat trafficking in persons that is facilitated by the criminal misuse of information and communications technologies, and to utilize technology to prevent and address such trafficking".[18]

Similarly, the 2013 Addendum to the OSCE Action Plan on Combating Trafficking in Human Beings recommends that OSCE participating States "promot[e] regular training courses, as appropriate, in accordance with national legal systems, for officials ... on all recent trends and aspects of THB, including ... the use of the Internet and other information and

12 See Melvin Kranzberg, "Technology and History: Kranzberg's Laws," *Technology and Culture 27.3* (Bulletin of Science, Technology and Society, 1 February 1995), vol. 15, No. 1, pp. 5–13.

13 See Thi Hoang, "The dual law of technology in trafficking" [website] (The Global Initiative Against Transnational Organized Crime, 23 July 2020). Available at: www.globalinitiative.net/analysis/leveraging-innovation-to-fight-trafficking-in-human-beings-a-comprehensive-analysis-of-technology-tools/ (accessed 21 October 2021).

14 See OSCE and Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools* (Vienna: OSCE and TAT, 22 June 2020).

15 See OSCE, UN.GIFT, *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime* (Vienna: OSR-CTHB, UN.GIFT, May 2010), p. 33.

16 See Patrick P. Belser, *Forced Labour and Human Trafficking: Estimating the Profits* (Geneva: ILO, March 2005), p. 17. The UN has estimated the total value of human trafficking at US$150 billion. See ILO, *Profits and Poverty: The Economics of Forced Labour* (Geneva: ILO, 20 May 2014), p. 13.

17 See Europol, *European Union Serious and Organised Crime Threat Assessment. Crime in the age of technology* (The Hague: Europol, 2017), p. 7.

18 See UNODC Commission on Crime Prevention and Criminal Justice, *Resolution 27/2, "Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies"* (Vienna: UNODC, 14–18 May 2018), p. 9.

communication technologies (ICTs) for committing THB related crimes, as well as training on the use of financial investigation techniques linked with THB related cases, and exchange of best practices".[19]

Less attention, however, has been paid at the national and international level to developing the necessary policy responses to technology-facilitated THB. By and large, countries have not taken steps to recognize technology-facilitated THB in their criminal statutes, updated criminal procedure codes or established the necessary industry standards on monitoring and reporting illegal content, mitigating risk or ensuring transparency. Instead, most countries have delegated regulation of the technology sector to the technology companies themselves. The result is a fragmented patch-work of policies and approaches that are ill-equipped to address the scale of the problem, the diversity of harms, and the sector-specific challenges that exist.

3. The paper

This report examines the different policy approaches taken by OSCE participating States to tackling the challenges posed by technology-facilitated THB.

In Part A, the paper begins by examining how technology has impacted the crime of THB and takes stock of how crises such as the COVID-19 pandemic have exacerbated an already grim state of affairs.

In Part B, the paper next explores how States have responded to technology-facilitated THB in their criminal statutes and criminal procedure codes, concluding that most countries need to expand and update their criminal procedures to account for the myriad challenges posed by technology-facilitated THB.

Part C examines the broader regulatory approach of countries to the technology industry in the context of THB, including the historical reliance on self-regulation and the recent, accelerating shift toward State-led regulation.[20] It examines efforts by the private sector and multi-stakeholder initiatives to improve the technology industry's response to technology-facilitated THB, and the successes and failures of the self-regulatory model. Part C concludes by looking at recent examples on how governments have begun to approach stronger, State-led regulation.

Part D examines central issues for policy makers in regulating the technology sector related to THB, including prevention measures such as age-verification, monitoring and reporting of prohibited content, content removal and blocking of websites, liability for online platforms, and transparency.

Part E presents the paper's final conclusions and a set of recommendations for policy makers to enhance safety, protect people online, and establish a clear and fair regulatory system for companies.

This paper is based on desk research and analysis of existing legislation and policies, as well as targeted interviews with representatives of law enforcement authorities and civil society organizations from OSCE participating States and Partners for Co-operation who are engaged in addressing the misuse of technology for THB purposes. While it draws conclusions and presents recommendations, the primary purpose of this report is to introduce the key considerations and myriad of issues faced by governments – as well as the technology industry and civil society – in addressing technology-facilitated THB from a policy perspective. The objective of the paper is to guide proactive, impactful policymaking that fosters safety for everyone and discourages online exploitation.

19 See OSCE, *Decision No. 1107 Addendum to the OSCE Action Plan on Combating Trafficking in Human Beings* (Vienna: OSCE, 6 December 2013), point 4.1, section II.

20 "Technology-facilitated trafficking" is understood for the purposes of this report as human trafficking offences (defined in line with the UN Protocol on Trafficking of Persons) that use digital technologies during any element of the offence.

PART A Introduction to technology-facilitated THB and the impact of crises on the problem

1. How information and communication technologies have changed the THB landscape

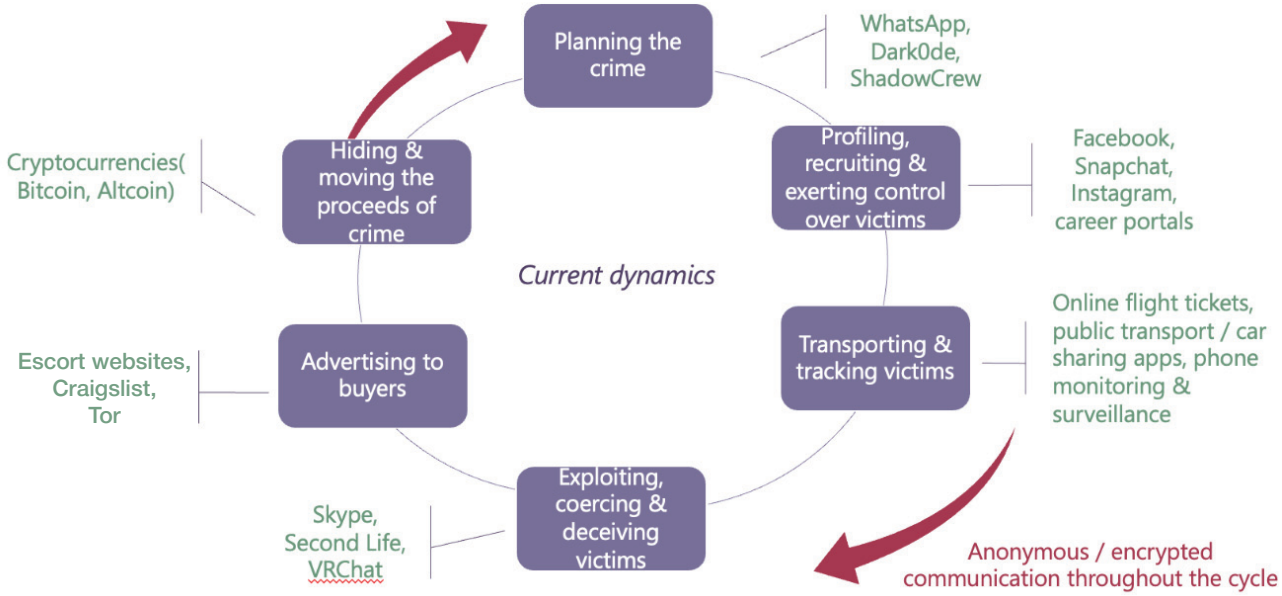
While ICT has enabled people to connect globally, it has also facilitated connectivity at a huge scale between THB perpetrators, their victims, and users of the services provided by victims. Indeed, technology has become ubiquitous within THB dynamics. Jessica Harrison, Operations Manager at the Modern Slavery and Trafficking Unit of the UK National Crime Agency has noted that traffickers have leveraged some form of digital technology in 100% of the sex trafficking cases reviewed by her unit the last three years.[21]

As noted in the below figure, ICT infiltrated every stage of the THB process:

a. **Planning the crime:** Traffickers use digital and network technologies such as encrypted apps to anonymously and securely plan and communicate with each other.

b. **Recruiting and exerting control over victims:** Traffickers use social media platforms like Facebook, Instagram, and VKontakte (Russian's largest social media platform) to profile, groom and recruit potential victims. In cases of sexual abuse, criminals use these platforms to study potential victims' posts to learn how to present themselves, for example as a boyfriend, a confidant, or an escape. In the case of labour exploitation, traffickers make use of career portals to post false job advertisements, or they actively roam social media platforms to scout for job seekers. Children and teenagers, especially girls, are specifically groomed and controlled through chat rooms, messaging apps and social networking sites like Facebook, Snapchat and KIK. Material that is sensitive due to its sexually explicit nature is repeatedly used to exercise control: traffickers threaten victims that if they do not follow the trafficker's instructions, the material will be shared with their family members and friends.

How technologies infiltrated the human trafficking landscape



Source: GI-TOC, 2021[22]

21 Telephone interview with Jessica Harrison, Operations Manager, Modern Slavery and Human Trafficking Unit, 19 November 2020.

22 See Global Initiative Against Transnational Organized Crime, *Preventing Vulnerability of and Strengthening Policy Responses For Commercial Sexual Exploitation Of Children In The Western Balkans* (working title), forthcoming.

c. **Exploiting, coercing and deceiving victims:** Traffickers use messaging/conferencing apps like Skype and online games like Second Life to coerce victims into being exploited, for example by sharing intimate images. In the case of sexual exploitation, sexual abuse is livestreamed, recorded, stored and distributed further.

d. **Advertising to buyers:** Traffickers use technologies to market their victims on various online platforms, both on the surface web and the dark web. Adult services websites play a core role in advertising the services of persons trafficked for sexual exploitation. However, the misuse of mainstream platforms like Facebook, Instagram, VKontakte, Odnoklassniki[23] and Twitter is also high.

e. **Distributing illicit materials:** Sexual exploitation material is distributed via peer-to-peer networks and stored in cloud applications such as Dropbox, Google Drive, OneDrive, etc. These materials are distributed via online social-media platforms like Facebook, Snapchat, KIK, Instagram, WhatsApp, etc. Livestreaming services such as Skype are also commonly used.

f. **Facilitating transportation and accommodation of victims of trafficking:** Perpetrators use technology to purchase travel tickets, or book temporary accommodation online. In many contexts, sex traffickers are known to regularly move victims between locations such as hotels or residences.

g. **Hiding and moving the proceeds of crime:** The emergence of cryptocurrencies such as Bitcoin and Altcoin has enabled traffickers to anonymously and securely receive their illegal proceeds, as well as to distribute funds between members of their criminal networks. Various reports also confirm that illicit funds from THB flow through the traditional financial services sector as well, often facilitated by technology.

A key additional concern in the context of sexually explicit material of persons trafficked online is that technology-based records of their exploitation (e.g., videos) often continue to be circulated online, even after the victim is recovered and the perpetrator convicted. This is commonplace in the context of the production of pornography and the (un-)known sharing of abusive material or live webcam videos. Most adult service sites do not require (meaningful) age verification for a person to upload pornographic videos or of the persons depicted in the material. Some sites allow content to be downloaded directly from the site; consequently, even if abusive material is removed by a company, it still can be shared with others or uploaded again.[24] The consequence of the persistent presence of online material depicting exploitation is the ongoing or repeated traumatization of victims.

Given the volume of data and number of online sites, traditional investigative techniques into abusive and exploitative material do not suffice for the online environment. Furthermore, as will be discussed later in this report, legislation and policies addressing these issues often lag well behind technological advancements, as well as behind traffickers' misuse of the technology. This further fuels the proliferation of technology-facilitated THB.

Online sexual exploitation of children

The internet has made it easier for children to be trafficked for sexual exploitation, whether it be through online grooming and recruitment or online sexual abuse. For example, according to the 2018 Thorn report *Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking*, technology is playing an increasing role in grooming and controlling child victims of sex trafficking in the United States. Before 2004, minors were advertised online in 38% of cases; this almost doubled by 2018, when online advertising of minors had increased to 75% of cases.[25]

A common pattern in some regions is for criminals to take advantage of economically deprived families by luring parents into exploitative activities, such as livestreaming sexual abuse of their children for payments.[26] The latter has been widely reported in Southeast Asian countries, where some

23 See Ministry of Internal Affairs of Moldova, *Information on the protection of children's rights in the Republic of Moldova on the theme "Information and communications technology and child sexual exploitation" pursuant to Human Rights Resolution 28/19 on the rights of the child*. Available at: www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj0uYexmLb0AhWIM-wKHW6ADSAQFnoECAsQAQ&url=https%3A%2F%2Fohchr.org%2FDocuments%2FIssues%2FChildren%2Fcommunications_technology%2FRepublicofMoldova.docx&usg=AOvVaw2iDSv9i9SWiujI8c-KPfki (accessed 21 October 2021).

24 See Nicholas Kristof, "The Children of Pornhub" [website] (*The New York Times*, 4 December 2020). Available at: www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html (accessed 21 October 2021).

25 See Thorn and Vanessa Bouche, Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking (Los Angeles: Thorn, January 2018), p. 7.

26 See Tech Against Trafficking, "The effect of COVID-19: Five impacts on human trafficking" [website] (Tech Against Trafficking, 16 April 2020). Available at: www.techagainsttrafficking.org/the-effect-of-covid-19-five-impacts-on-human-trafficking/ (accessed 21 October 2021).

parents might not even perceive online child sexual exploitation (CSE) as harmful to their children, since there is no physical interaction involved. Such illicit activity is made easier by the existence of a large number of persons willing to pay to view online child sexual abuse and the minimal investment required: in order to commit the crime, all that is needed is an internet connection, a smartphone with a camera and microphone, and a platform to receive financial payments. This makes it easier to access, download, produce and share child sexual exploitation material (CSEM) online.

The expansion of the THB marketplace discussed above is particularly tangible in the context of online CSEM. The volume of CSEM identified globally has increased exponentially in recent years – from more than one million reports of CSEM in 2014 to 18.4 million reports in 2018. These reports contained over 45 million online photos and videos of children being sexually abused – more than double the number of those found in 2017.[27]

Online child CSE is often addressed by tailored policy and legal instruments, and there are arguments for addressing online CSE as a separate crime from that of THB. However, in many cases, online CSE falls within the definition of THB set out in the Palermo Protocol – i.e., it contains an "action" (e.g. recruitment or harbouring) for an exploitative purpose (a means is not required when the victim is a child). Court decisions across a range of OSCE participating States have found online CSE to meet the elements of THB.[28] Consequently, online CSE is one of the THB phenomena explored within this report.

2. The impact of crises on technology-facilitated THB

Countries are not always able to design their anti-trafficking systems to respond to major developments that take place at national, regional or global levels, regardless of the available resources. Unpredictable crisis situations can happen, and they can have a major impact on anti-trafficking systems, with the most significant recent example being the impact of the COVID-19 pandemic on anti-trafficking systems.[29]

The COVID-19 pandemic, and the ensuing restrictions imposed upon in-person interaction, shifted many activities online; the THB marketplace was no exception. Children's online vulnerabilities and increased digital presence are major attack vectors that traffickers have been increasingly exploiting during the pandemic. Prominent law enforcement agencies such as Europol and the FBI have issued warnings to parents and teachers about increased risks of online child exploitation: according to the FBI "offenders may make casual contact with children online, gain their trust, and introduce sexual conversation that increases in egregiousness over time".[30]

These dynamics have played out at the national and regional levels. During the COVID-19 pandemic, Europol reported a spike in demand for online child sexual exploitation and distribution of CSEM in many parts of Europe, as more predators and potential perpetrators were confined at home. For example, German authorities reported that cases involving child sexual abuse images online doubled during the pandemic.[31] The Swedish National Police also reported an increase in the sharing of CSEM online following the introduction of lockdown measures.[32] Similarly, Spain and Denmark reported an increase in the number of reports of CSEM online and attempted access to illicit websites and forums containing CSEM. Spain noted a 25% increase in peer-to-peer downloads of CSEM over the last two weeks of March 2020.[33]

27 See Michael H. Keller and Gabriel J.X. Dance, "The internet is overrun with images of child sexual abuse. What went wrong?" [website] (The New York Times, 29 September 2019*). Available at:* www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html (accessed 21 October 2021).

28 See National Criminal Investigation Service (NCIS) of Norway, Human Trafficking in Norway — Criminal A*ctors: A Situational Picture Based on Police Sources* (Oslo: NCIS, 20 December 2017), p. 23.

29 See OSCE/ODIHR and UN Women, *Guidance Addressing Emerging Human Trafficking Trends and Consequences of the COVID-19 Pandemic* (Warsaw: OSCE, 30 July 2020).

30 See Federal Bureau of Investigations, "School closings due to COVID-19 present potential for increased risk of child exploitation" [website] (Washington D.C.: FBI, 23 March 2020). Available at: www.fbi.gov/news/pressrel/press-releases/school-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation?utm_campaign=email-Immediate&utm_medium=email&utm_source=national-press-releases&utm_content=%5B795639%5D-%2Fnews%2Fpressrel%2Fpress-releases%2Fschool-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation (accessed 21 October 2021).

31 See DW, "Germany: Crimes involving child sexual abuse images almost double" [website] (DW, 7 November 2021). Available at: www.p.dw.com/p/42h75 (accessed 20 November 2021).

32 See NetClean, "What Happens To The Consumption Of Child Sexual Abuse Material When Millions Of People Work From Home?" [website] (NetClean, 3 April 2020). Available at: www.netclean.com/2020/04/03/what-happens-to-the-consumption-of-child-sexual-abuse-material-when-millions-of-people-work-from-home/ (accessed 21 October 2021).

33 See Europol, *Catching the virus cybercrime, disinformation and the COVID-19 pandemic* (The Hague: Europol, 3 April 2020), p. 8.

Other law enforcement agencies reported that the already high number of CSEM tripled in 2020, following the start of the pandemic.[34] Given that 2021 was recently reported to be the worst year on record for online child exploitation[35], the accelerated download and sharing of exploitative material could point towards a permanent expansion of the CSEM market.

During periods of increased demand for CSEM, existing child victims might be exposed to greater frequencies of violence and exploitation, especially when the abusers are their own caregivers, and when home is not a safe place for them.[36] Moreover, as is the case for adult victims of trafficking, child victims and survivors might find their access to protection, legal and rehabilitation services reduced or cut off due to lockdown measures. Furthermore, given the increased sharing and distribution of CSEM, child victims and survivors may experience earlier abuse materials still being circulated and distributed on the internet, and at a faster pace and higher volume, thus leading to further traumatization.

It is not only trafficking in children that has moved further online during the COVID-19 pandemic. Trafficking of adults has also undergone similar shifts in response to offline movement restrictions. Adult services websites, reported in many countries to be the type of e-platform most targeted by traffickers, are expanding in size and diversifying their services. Since traffickers can easily utilize such sites, their expansion is believed to increase the risks for exploitation.[37] Another example is the introduction by adult services websites in the UK of webcam services. This type of service has reportedly been used to exploit THB victims.[38]

An important piece of this evolving landscape is the impact of the pandemic on the response to THB. One worrying trend observed during the pandemic's lockdown measures is the private sector's decreased cybersecurity and human monitoring capacities related to digital services or platforms they offer or manage, especially social media. Social media companies like Facebook, Twitter and Youtube have reduced their in-office moderators during the pandemic and temporarily increased reliance on monitoring algorithms to moderate content on their platforms.[39] This shift has reportedly been associated with decreased human oversight and longer delays in reviewing potentially harmful content, raising security and accuracy concerns related to these service providers' policing algorithms. This decreased cyber security and human monitoring capacity, coupled with an increase in digital presence of children online, as discussed above, creates opportunities for traffickers.

While some companies agree that their contingency plans included relying more on artificial intelligence, they report that this actually led to an increase in the number of removals of prohibited content, with the result that more content was removed rather than less. As a result, the companies note, there were more appeals and technology companies prioritized human review to resolve those appeals. However, this situation highlights that automated monitoring is not a perfect, stand-alone solution.

Likewise, the response of governments has been impacted. Although the COVID-19 pandemic has reportedly led to a surge in demand that has fostered online sexual exploitation of both children and adults, the prosecution rate of such illicit activities reportedly dropped by 90% as resources were redirected and in-person court proceedings and investigations slowed dramatically or even closed down.[40] Thus, as traffickers were shifting online, private sector and law enforcement online efforts actually contracted.

In short, the COVID-19 pandemic has disrupted some traditional forms of THB, but it has also exacerbated the THB risks of both existing victims and vulnerable groups. Recent experience demonstrates that such crises can prompt shifts in the modes and venues of exploitation that are challenging to address; likewise, they can disrupt the anti-trafficking response across investigation and prosecution, protection, prevention and partnerships. The COVID-19 pandemic, and its resulting social, political and economic crises, has shown that policymakers are generally not prepared to respond quickly to such abrupt shocks and their consequences in society. Meanwhile, human traf-

34 See Valiant Richey, OSCE, "Opinion: Invisible crimes like human trafficking rise during COVID-19" [website] (Thomson Reuters Foundation News, 16 December 2020). Available at: www.news.trust.org/item/20201216122708-84btm (accessed 21 October 2021).

35 See Dan Milmo, "2021 was worst year on record for online child sexual abuse, says IWF" [website] (The Guardian, 13 January 2022). Available at: https://www.theguardian.com/society/2022/jan/13/2021-was-worst-year-on-record-for-online-child-sex-abuse-says-iwf (accessed 25 January 2022).

36 See UN News, "Children vulnerable to abuse and violence during coronavirus lockdowns, UN experts warn" [website] (United Nations, 7 April 2020). Available at: www.news.un.org/en/story/2020/04/1061282 (accessed 21 October 2021).

37 See Harriet Grant, "Urgent action needed as rise in porn site traffic raises abuse fears" [website] (The Guardian, 25 March 2020). Available at: www.theguardian.com/global-development/2020/mar/25/urgent-action-needed-as-spike-in-porn-site-traffic-raises-abuse-fears-say-mps (accesses 21 October 2021).

38 Telephone interview with Jessica Harrison, Operations Manager, Modern Slavery and Human Trafficking Unit, 19 November 2020.

39 See Elizabeth Dwoskin and Nitasha Tiku, "Facebook sent home thousands of human moderators due to the coronavirus. Now the algorithms are in charge" [website] (The Washington Post, 24 March 2020). Available at: www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/ (accessed 21 October 2021).

See also Human Rights Watch, "COVID-19 and children's rights" [website] (Human Rights Watch, 9 April 2020). Available at: www.hrw.org/news/2020/04/09/covid-19-and-childrens-rights-0#_Toc3725653 (accessed 21 October 2021).

40 See Valiant Richey, OSCE, "Opinion: Invisible crimes like human trafficking rise during COVID-19" [website] (Thomson Reuters Foundation News, 16 December 2020). Available at: www.news.trust.org/item/20201216122708-84btm (accessed 21 October 2021).

fickers have shown once again their ability to adapt. Assisted by the shift in resources and priorities towards virus containment measures, traffickers have nimbly exploited the efficiency of online platforms, as well as reduced monitoring and policing capabilities from law enforcement and the private sector, to maintain their business model.[41]

In conclusion, when countries are in the face of sudden, major crises that can lead to increased vulnerabilities and increased risks of exploitation, policymakers have to be agile and rapidly design policy solutions that can diminish the negative impact of crises. The deliberative nature of policy adoption can make this a difficult task, but there are always basic actions that authorities can take to prevent or mitigate exploitative situations during crises. Advance planning is one important element that can ease the burden of short-term crisis response. Adequate and sustainable funding of anti-trafficking response systems and strong institutional frameworks can also help mitigate the impacts of crises.[42]

41 See Livia Wager and Thi Hoang, *Aggravating circumstances: How coronavirus impacts human trafficking* (Global Initiative against Transnational Organized Crime, May 2020), p. 24.

See also Roop Sen and Uma Chatterjee, "Lockdown provokes bad memories for trafficking victims" [website] (rediff.com, 18 April 2020). Available at: www.rediff.com/news/column/how-trafficking-victims-dealwith-the-lockdown/20200418.htm (accessed 21 October 2021).

42 See OSCE/ODIHR and UN Women, *Addressing Emerging Human Trafficking Trends and Consequences of the COVID-19 Pandemic* (Warsaw: OSCE, 30 July 2020), p. 111.

PART B Addressing technology-facilitated THB in criminal justice legal frameworks

Legal frameworks often lag behind technological innovations, leaving legislative loopholes and gaps, as well as insufficient understanding of evolving challenges that require specific solutions. In the case of THB, this deficiency has fostered a sense of impunity for traffickers, encouraging perpetrators to perceive the crime as low risk and high reward. It also makes technology-facilitated THB more difficult to investigate and prosecute[43] because legal frameworks do not always account for evolving criminal landscapes and the ability of criminals to mainstream technology in their operations. For example, widespread stringent data protection legislation, and the overall drive for enhanced privacy for individuals online, can pose a substantive challenge to investigations of technology-facilitated THB that often require access to personal data. As the pivotal role of technology in most, if not all, THB cases is increasingly recognized, countries are beginning to closely examine the issue and, in limited cases, introduce reform in their legal systems to address the challenges that responding to technology-facilitated THB brings.

This section considers how countries have responded to technology-facilitated THB through laws and policies in their criminal justice systems, specifically: 1) how legislation has defined the THB offense in criminal law and whether technology-facilitated THB is captured implicitly or explicitly; and 2) whether States' criminal procedures cover the investigation and prosecution of technology-facilitated THB offences, including the collection and use of electronic evidence in prosecutions. In particular, the paper highlights trends in approaches adopted by OSCE participating States, together with contrasting positions or points of ongoing debate.

1. Technology-facilitated THB in international law and national legislation

a. Legislation criminalizing THB

Broadly, current international and regional legal frameworks criminalizing THB – ranging from the Palermo Protocol to instruments covering forms of child labour, forced labour, slavery and other overlapping areas – do not explicitly recognize the role of technology in facilitating human trafficking.[44] There is an ongoing discussion within literature, among the legal and law enforcement practitioners in OSCE participating States interviewed in the framework of this report, and between policy makers as to whether explicitly including technology as a facilitator/enabler in international and national legal frameworks is needed and could enhance effective investigation and prosecution of technology-facilitated THB offences, or whether existing definitions are sufficiently flexible and do not require amendment.

For example, some international bodies, including the Committee on the Elimination of Discrimination Against Women (CEDAW), have noted that "the realities of trafficking … extend beyond the scope of the United Nations Trafficking Protocol." The CEDAW emphasizes "the recent trends and the role of information communication technology, social media and chat apps in the recruitment of women and girls and their exploitation" and has called for legal frameworks to "[address] contemporary methods of trafficking, including those using information and communications technologies, including social media."[45] In a contrasting position, the Council of Europe emphasizes the flexibility of the definitions in the Protocol, arguing instead that technology can

43 See OSCE, "Statement by Ambassador Petra Schneebauer, National Co-ordinator for Combating Trafficking in Human Beings, Austria, 19th Alliance against Trafficking in Persons: Panel 1" [website] (Vienna: OSCE, 18 April 2019), starting from 19:10 Available at: www.osce.org/cthb/419933 (accessed 21 October 2021).

44 The key international instrument criminalizing human trafficking offences, the Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, defines trafficking as the recruitment, transportation, transfer, harbouring or receipt of persons by the threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or of a position of vulnerability or of the giving or receiving payments or benefits with the purpose of exploitation. While technology can be used in any stage of the crime, it is not explicitly included in the above definition, or indeed at any point in the Palermo Protocol. The supporting international instruments, covering forms of child labour, slavery, and other overlapping areas, are similarly silent on the use of technology, as are regional instruments such as The Council of Europe Convention on Action against Trafficking in Human Beings.

45 See Committee on the Elimination of Discrimination against Women, *Convention on the Elimination of All Forms of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration* (United Nations, 6 November 2020), p. 20.

be part of the commission of any element of the offence, and does not require explicit recognition.[46]

The predominant approach among the OSCE participating States is to apply THB frameworks originally crafted for "offline" contexts to technology-facilitated THB offences without express references to technology in the statutory definition of the crime. This approach was reflected in conversations with practitioners: stakeholders contacted during the research for this report, including national law enforcement bodies operationally tasked with investigating and prosecuting technology-facilitated THB offences, largely opined that the existing definitions of THB in their national legislation were sufficiently broad to apply to the wide range of contexts in which technology operates as an enabler. They generally did not perceive the lack of explicit reference to technology in legislation as a barrier to operations. For example, in support of this perspective, representatives from the Cyber Crimes Unit of Israel (an OSCE Partner for Co-operation) reported that two recent cases involving livestreaming of sexual abuse – where technology played a core role in committing the crime – were successfully prosecuted under Israel's Penal Code as sex trafficking offences, even though the Israeli Penal Code does not expressly include technology as an enabler to those offences.[47]

Further, the risk of becoming quickly outdated is an ever-present challenge to legislation related to technology at large. Incorporating explicit references to technology as an enabler into legislation would need to be sensitive to the risk of unintentionally excluding possible uses of technology. Drafting approaches such as that adopted in the EU General Data Protection Regulation, which are based on principles together with more detailed provisions, have been designed to mitigate this risk. Using principles in legal definitions ensures that potential developments in technology misused for trafficking purposes will not obviate the application of relevant laws and thus will not disrupt the legal process.

On the other hand, incorporating an explicit reference to technology as an enabler was perceived by some stakeholders as a valuable tool for enhancing awareness of the central role played by technology in the committing of THB offences. In support for this approach, Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation, highlighted the norm-building aspects of legislation: "People are educated by the statute". Pinter cited the recent inclusion of leveraging drug addiction as a form of coercion into THB provisions, noting that it had greatly enhanced awareness of this widespread practice, facilitating prosecution, despite the fact that such forms of coercion technically fell within the scope of the THB statute prior to its amendment. Pinter concluded that expressly including technology as an enabler could, in an analogous way, "help courts and everyone understand that traffickers use the internet as a tool". Similarly, law enforcement in Kazakhstan opined that THB offences should explicitly provide for combating recruitment of victims via ICT.[48] Importantly, referencing technology-facilitated THB would also serve to rebut any potential claim that a lack of explicit reference to technology in offences constitutes an implicit exclusion of technology-facilitated offences.

A growing number of strategic and policy frameworks explicitly emphasize the role of technology as an enabler in committing THB offenses (see Annex 1). Some examples in practice from the OSCE region draw attention to technology-facilitated THB in the legal framework. For example, the Criminal Code of the Republic of Moldova expressly indicates information and communication technologies as a means to groom children including for sexual exploitation purposes. In the same context, the State of Washington in the U.S. had a crime called "communicating with a minor for immoral purposes" which was roughly equivalent to "grooming." With the rapid development of internet and increasing instances of online grooming, the State amended the statute to provide that if the communicating was done online it became a felony (instead of a misdemeanour).[49] This was done both as a deterrent and to incentivize law enforcement to pay increased attention to the misuse of internet for sexual exploitation of children.

In many jurisdictions, policymakers could alternatively adopt interpretive guidance to explain that the legal THB definitions featured in laws include technology-facilitated THB within their scope, to facilitate application of the law to such offences and ensure the laws are applied coherently. In this way, although the formal definition of THB does not make reference to technology-facilitated exploitation, interpretative guidance could bring more clarity to practitioners – including courts – and serve as a way to apply consistent standards in criminal justice processes.

46 See Council of Europe, *Explanatory Report to the Council of Europe Convention on Action against Trafficking in Human Beings* (Warsaw, 16 May 2005), p. 15, para 79.

47 Telephone interview with Ayelet Dahan, Deputy Anti Trafficking Coordinator, Ministry of Justice of Israel, and Alexandra Karra, *Senior Attorney*, *Cybercrime Department*, State Attorney's *Office*, *Ministry* of Justice of Israel, 19 November 2020. Note that both cases involved trafficking in children, but were prosecuted as sex trafficking offences (not under tailored CSE legislation).

48 See IOM, *Study Report Exploring the Role of ICTs in Recruitment for Human Trafficking in the Republic of Kazakhstan, the Kyrgyz Republic and the Republic of Tajikistan* (Astana: IOM, 2019).

49 See Washington State Legislator, "RCW 9.68A.090 Communication with minor for immoral purposes—Penalties." [website]. Available at: www. app.leg.wa.gov/rcw/default.aspx?cite=9.68a.090. (accessed 21 October 2021).

b. Cyber-crime legislation

In the same way that most national and international anti-trafficking legal frameworks do not expressly reference technology-facilitated THB, international frameworks governing cybercrime – another key corpus of law relevant in addressing technology-facilitated THB – do not explicitly incorporate references to THB, in particular of adults. This includes the Council of Europe Convention on Cybercrime (the "Budapest Convention"), the most widely ratified instrument relating to cybercrime.[50] The focus of the Budapest Convention is on harmful activity conducted through the internet, protecting the integrity of computer systems, and data. However, although it mandates the criminalization of the production, offer, distribution, procurement and possession of child abuse and sexual exploitation on a computer system, it does not address a broader set of illicit activity conducted using information technologies, including THB offences involving adult victims.[51]

The EU Parliamentary Assembly's comments on the draft of the Budapest Convention recommended expansion of "content offences" to include "the use of the Internet for human trafficking purposes", or alternatively the immediate drafting of a protocol titled "Broadening the scope of the convention to include new forms of offence" to include "the use of the Internet for trafficking in human beings", alongside a number of other offences.[52] However, the final draft limited content offences to child sexual abuse material online, excluding adult THB offences from the scope of the regulatory framework. Further, while an additional Protocol to address offences relating to racism was published, and a second additional Protocol seeking to enhance international co-operation in the investigation of cybercrime is in the process of being drafted, there has been no parallel drive towards such a Protocol regarding THB.

Likewise, in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse ("Lanzarote Convention") there is a focus on the role of ICT both in provisions requiring criminalization of "knowingly obtaining access, through information and communication technologies, to child pornography", and in provisions relating to the investigation of technology-facilitated offences. However, there are no express provisions on trafficking. [53]

The international attention on ICT being used to commit child abuse offences is reflected in the national legislation of a number of OSCE participating States. For example, 2017 amendments to the US Crimes and Criminal Procedure Code explicitly introduced recognition of the role of ICT in "producing a visual depiction" of child sexual abuse, "or transmitting it live" (although the role of technology is not explicitly addressed with regard to other phases of the crime, including recruitment).[54] Similarly, Moldova's Criminal Code expressly notes that the production and distribution of child sexual abuse material is an offence, including when in "electronic form".[55]

One likely factor in the different approaches to child sexual exploitation online and adult online trafficking offences is greater policymaker consensus on the former as a policy priority.[56] Extensive lobbying from media and civil society has also likely played a role in securing significant focus on ICT in the context of child sexual exploitation online. Further, determining that content is illegal is more difficult when it involves an adult, further complicating legislative approaches.

The accelerating use of technology in THB presents a stronger case for explicitly including THB in the Budapest Convention than when it was originally drafted. International deliberations surrounding the regulation of cybercrime are in the initial phase only and – given the extended process of international negotiations and consensus-building among a large number of countries on such legal instruments – it is difficult to say with certainty when substantive progress will be achieved in this direction.[57] Given the increase in technology-facilitated THB, action could help provide legal certainty regarding technology-facilitated THB,

50 Other international frameworks such as the Africa Union Cybercrime Convention, the League of Arab States Convention, the CIS Agreement, and the SCO Agreement also do not explicitly incorporate references to THB, in particular of adults.

51 See Marc D. Goodman and Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace" (*International Journal of Law and Information Technology* 10/2, 2002), p. 10.

See also UNODC, *Comprehensive Study on Cybercrime, Draft* (New York: United Nations, 2013), p. 16, which identified 14 "acts commonly included in notions of cybercrime" in national and international instruments. These include offences relating to child sexual abuse and terrorism, but exclude adult human trafficking offences.

52 See Council of Europe, Committee on Legal Affairs and Human Rights, *Report 15379 on the Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (Council of Europe, 28 September 2021), p. 5, section 2B.

53 See Council of Europe, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote: Council of Europe, 25 October 2007), p. 8 and p. 12.

54 Amendment to section 2551 of the title 18 ("Crimes and Criminal Procedure") US Code was introduced to criminalize those who knowingly employ, use, persuade, induce, entice or coerce – or assist someone else to do the same conduct – any minor to engage in or transport any minor with the aim of such minor engaging in sexually explicit conduct for the purpose of producing a visual depiction of such conduct or transmitting it live.

55 See Parliament of Moldova, Criminal Code of the Republic of Moldova, Nr. 986, 18 April 2002 (Official Monitor Nr. 72-74, art. 195, 14 April 2009), article 208.

56 See Marc D. Goodman and Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace" (*International Journal of Law and Information Technology* 10/2, 2002).

57 See UNODC, Ad hoc committee established by General Assembly resolution 74/247 [website] (UNODC). Available at: www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed: 21 October 2021).

including regarding its definition, and reverse the high-reward low-risk calculation being utilized by traffickers. As international consensus on a global cybercrime convention remains elusive, regional co-ordination of legislative approaches, including in the framework of the Budapest Convention, could be a solution to avoid piecemeal national efforts.

2. Criminal procedure: investigation and prosecution of technology-facilitated THB

In the research conducted for this report, national law enforcement authorities cited a number of procedural challenges in conducting investigations of technology-facilitated offences – ranging from obtaining evidence, to cross-border e-evidence sharing and using e-evidence in trial – as critical considerations for responding to technology-facilitated THB.[58] Stakeholders in OSCE participating States further noted that online investigations are hampered by "tighter regulations" than their offline counterparts, with data protection considerations often posing significant challenges.[59]

The intersection of technology and criminal procedure continues to be an area of legal reform in national and international frameworks. For example, with regard to CSE, both the Budapest and Lanzarote Conventions emphasize the need for procedural reform enabling effective investigation and prosecution of child sexual exploitation facilitated by information and communication technologies (ICT).[60] Currently, consultations are progressing on the Second Additional Protocol to the Budapest Convention which specifically seeks to enhance international co-operation in online investigations.[61]

a. Information-sharing between companies and law enforcement

The Budapest Convention requires signatories to adopt legislative measures to empower authorities to issue production orders to internet service providers; some OSCE participating States such as Albania, Germany and the Netherlands[62] have introduced such provisions.[63] In Kazakhstan, 2019 legislative amendments enabled law enforcement to demand subscriber data from mobile operators – a reform expected to facilitate the identification of individuals involved in the recruitment of victims of THB, in which ICT has been identified as playing a central role.[64] And those with existing frameworks continue to modify them over time. Illustratively, a bill currently awaiting enactment in Germany specifically amends existing legislation to simplify court enforcement of data sharing requests of internet service providers.[65]

There do, however, remain countries that lack regulatory frameworks governing the collection and use of digital evidence,[66] or where frameworks continue to be premised at least in part on voluntary data sharing.[67] Moreover, because the Budapest and Lanzarote Conventions do not address THB of adults, the adoption of a second protocol will not solve the existing challenges at the international level.

Where regulatory frameworks exist at the national level, in many jurisdictions there remains a lack of clarity in the information sharing duties of such service providers. For example, although Estonia's Information Society Services Act requires information society service providers to "promptly inform the competent supervisory authorities of alleged illegal activities undertaken or information provided by recipients of their services",[68] there is little clar-

58 Written submissions by Anu Leps, National Coordinator against Trafficking in Human Beings, Ministry of Justice, Estonia, 09 October 2020.

See also UNODC, *Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, "Comments received in accordance with the Chair's proposal for the work plan for the period 2018-2021"* (UNODC, 16 March 2018), p. 21.

59 Written submissions by Anu Leps, National Coordinator against Trafficking in Human Beings, Ministry of Justice, Estonia, 09 October 2020.

60 See the Council of Europe, *Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse* (Lanzarote, 25 October 2007), article 30.

61 See the Council of Europe, "Protocol negotiations of a draft Second Additional Protocol to the Convention on Cybercrime" [website] (Council of Europe). Available at: www.coe.int/en/web/cybercrime/t-cy-drafting-group (accessed 21 October 2021).

62 See UNODC, *Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, "Comments received in accordance with the Chair's proposal for the work plan for the period 2018-2021"* (UNODC, 16 March 2018), p. 10.

63 These are often in the same regulatory frameworks that set out "notice and take down procedures", whereby states can compel online platforms to remove content.

64 See Mayya M. Rusakova, *Study Report. Exploring the Role of ICTs in Recruitment for Human Trafficking in the Republic of Kazakhstan, the Kyrgyz Republic and the Republic of Tajikistan* (International Organization for Migration, 2019), p. 22.

65 See Dr. Alexander Hardinghaus, Ramona Kimmich and Sven Schonhofen, "German government introduces new bill to amend Germany's Hate Speech Act, establishing new requirements for social networks and video-sharing platforms" [website] (Technology Law Dispatch, 6 April 2020). Available at: www.technologylawdispatch.com/2020/04/regulatory/german-government-introduces-new-bill-to-amend-germanys-hate-speech-act-establishing-new-requirements-for-social-networks-and-video-sharing-platforms/ (accessed 21 October 2021).

66 Written contribution by the competent authorities of Montenegro, 06 October 2020.

67 For example, in Georgia co-operation remains to some extent governed by a 2010 Memorandum of Understanding concluded between Law Enforcement Agencies and Internet Service Providers (ISPs) in which ISPs undertook to cooperate and share information with law enforcement agencies for the purpose of conducting investigations in accordance with Georgian legislation. Although Memoranda can shape the framework for co-operation, they do not typically create a legal requirement on their parties.

68 See Parliament of Estonia, Information Society Services Act (RT I 2004, 29, 191, 14 April 2004), section 11(3).

ity surrounding what constitutes "illegal activities", and a similar lack of detail regarding how individuals should notify the online platforms.[69]

Further, even where such frameworks do exist, obtaining evidence can still remain a challenge. Some States noted procedural complexity as a key obstacle. In Israel, although a process of court-issued warrants for the collection of electronic evidence is in place, such warrants are challenged in court far more commonly than their offline counterparts, and there remain a number of unresolved issues in the use of warrants for electronic evidence. For example, it is unclear whether authorities in possession of a warrant can use reasonable force to compel an individual to unlock their phone, either by sharing the code or using their fingerprint.[70] Meanwhile, stakeholders operating within prosecutorial roles in the United States cited a lack of political will, both at the level of the State and in the private sector, as the key obstacle in obtaining data from online platforms for conducting THB investigations.[71] Stakeholders also report a lack of responsiveness on the part of online platforms as a challenge in obtaining data.[72]

The Draft 2021 National Strategy for Child Exploitation Prevention and Interdiction ("the Draft Strategy") recently issued by the US Department of Justice highlighted a number of these issues as barriers to successful investigation and prosecution of online child exploitation cases. For example, in noting the extremely high volume of cyber tips received by law enforcement and the need for greater quality of information in the tips, the Draft Strategy notes that "there is a system in place for the three main players involved – the tech industry, NCMEC [US National Center for Missing & Exploited Children], and law enforcement – to share information about the quality of the information being shared…." The Draft Strategy goes on to state that "Congress may need to consider enacting legislation to facilitate this necessary process improvement." At the same time, while representatives of the technology companies recognize the importance of providing detailed, reliable and actionable cyber tips, they assert that legislating in this area could restrict adaptation in a fast evolving technological environment and could be ineffective in the medium term.

The Draft Strategy also echoes the concerns raised regarding systematic issues related to obtaining evidence through legal process, observing that "both law enforcement agencies and the tech industry are dissatisfied with the situation concerning child exploitation search warrants." The Draft Strategy highlights law enforcement frustration with the failure of companies to respond to warrants, delays in receiving information, and company-initiated litigation of the warrants. These issues are compounded when the relevant company resides outside the jurisdiction. The Draft Strategy also notes that the lack of uniformity in terminology or process is challenging for companies.

b. Removing and retaining unlawful content

A further challenge in obtaining the required evidence in investigations of technology-facilitated THB is the fact that online platforms commonly delete unlawful content that is reported to them or that they identify as illicit in their own due diligence investigations.

In their recommendation on the roles and responsibilities of internet intermediaries, the Committee of Ministers of the Council of Europe emphasized that intermediaries taking down content related to serious crime, either in response to requests or in line with their own content removal policies, should retain such material to facilitate criminal investigations.[73]

Regulatory frameworks in many OSCE participating States, including for example Albania, Moldova and Ukraine, explicitly require that internet service providers (ISPs) retain data for a set period of time to enable investigations.[74] However, in practice many platforms continue to delete the content they restrict access to – this has posed vast and ongoing investigative challenges across a range of criminal investigations, including into war crimes, the illicit wildlife market, illicit trade in art and antiquities, as well as technology-facilitated human trafficking, particularly

69 Written submissions by Anu Leps, National Coordinator against Trafficking in Human Beings, Ministry of Justice, Estonia, 09 October 2020. Information Society Services Act § 11, www.riigiteataja.ee/en/eli/515012019001/consolide.

70 Telephone interview with Ayelet Dahan, Deputy Anti Trafficking Coordinator, Ministry of Justice of Israel, and Alexandra Karra, *Senior Attorney*, *Cybercrime Department*, State Attorney's *Office*, *Ministry* of Justice of Israel, 19 November 2020.

71 Telephone interview with Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation, 8 December 2020.

72 See Leonie Cater, "How Europe's privacy laws are failing victims of sexual abuse" [website] (Politico, 13 January 2021). Available at: www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/ (accessed 21 October 2021).

73 See Council of Europe, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries* (Council of Ministers, 7 March 2018).

74 See Albania Criminal Procedure Code, Art 191a, 208a, 221-223, 299a, 299 b. Regarding Ukraine, although Ukraine had pre-existing data retention obligations in the "Law on Telecommunications", the updated "Law on Electronic Communications" initially removed the obligation on internet service providers to retain data for the purpose of criminal investigations. However, on 1 September 2020, MPs laid draft law 4003 on amendments to the Criminal and Administrative Procedure Codes to parliament which, *inter alia*, re-introduced retention obligations on internet service providers to store information in digital form, including traffic data, for a period of 12 months. Regarding Moldova, see Article 7 (f) of the Law 20/2009 on preventing and combating cybercrime.

of adults.[75] There are different reasons for this situation. For example, the Draft Strategy discussed in the previous section notes that even though companies in the United States are required to preserve data related to child exploitation, some companies do not preserve it after giving notice to law enforcement, under the belief that submission of the cyber tip is sufficient preservation of the data.

c. Covertly accessing devices

Although the Budapest Convention dictates that States should legislate powers to search computer networks, as well as collect, intercept and retain communications data, historically States have not provided sufficient legal protocols on how to carry out such procedures at the national level. However, a growing number of OSCE participating States, including Germany, Italy, the Netherlands, Spain and the UK, have introduced legislation allowing law enforcement to access suspects' computers when investigating technology-facilitated offences, including THB.[76] These frameworks grant law enforcement the power to access greater amounts of information without relying on co-operation by private sector companies.[77] Such powers have a longer history in the context of counter-terrorism operations, however, their extension to investigations for a broader set of serious crimes, including THB offences, is more recent and growing. This evolution was a reaction to fears among law enforcement that they were increasingly unable to access information necessary for investigations. Typically, strict procedural requirements, such as mandatory court orders enabling hacking, limit when such powers can be used.[78]

By covertly "hacking" devices, law enforcement can capture specific elements of data, monitor computer use, and search stored data, among other functionalities. In Germany, 2017 amendments to the Code of Criminal Procedure provided a legal basis for police hacking in criminal investigations (powers that previously had been reserved for anti-terrorism investigations)[79] that also enable covert online surveillance in cases of THB.[80] Similarly, the covert surveillance and hacking powers of Dutch law enforcement conducting investigations into serious crimes (including THB) were significantly expanded by the enactment of the Dutch Computer Crime Act II, which entered into force in March 2019. The Computer Crime Act also facilitates online investigations into grooming offences (focusing on child sexual exploitation and trafficking) by enabling officers to "lure" perpetrators by posing as underage children. Earlier case law rendered such practices unlawful.[81]

In Spain, 2015 amendments to the Criminal Procedure Code, which strengthened technology-related investigations including undercover surveillance of communication channels, expressly identified THB and trafficking of organs as crimes that can be investigated using the specialized investigative techniques set out therein. [82] In the United States, law enforcement agencies have used such "networking investigation techniques", bypassing anonymity protections of certain forms of software or leveraging vulnerabilities in encryption, to take down a number of surface and darknet websites containing child sexual abuse material.[83]

A second wave of countries, including Ukraine, are currently in the process of drafting and enacting legislation to harmonize procedures for online investigative techniques for technology-facilitated criminal offences, the collection of electronic evidence, and the use of electronic evidence in prosecutions.[84]

75 See Global Initiative Against Transnational Organized Crime, "Research findings from Digital Disruption programme on the Illegal Wildlife Trade" [website] (GI-TOC, 05 October 2018). Available at: www.globalinitiative.net/initiatives/digital-dangers/ (accessed 21 October 2021).

See also Global Initiative Against Transnational Organized Crime, "Presentation by Katie A. Paul, Co-Director of the Antiquities Trafficking and Heritage Anthropology Research (ATHAR) Project during "Culture in Ruins: The illicit trade in cultural property in North and West Africa", ENACT, 26 November 2020". Available at: www.globalinitiative.net/analysis/culture-in-ruins-the-illicit-trade-in-cultural-property-in-north-and-west-africa/ (accessed 21 October 2021).

76 See Ivan Škorvánek , Bert-Jaap Koops , Bryce Clayton Newell , and Andrew Robert, *"My Computer Is My Castle":*

New Privacy Frameworks to Regulate Police Hacking (Tilburg Institute for Law, Technology, And Society, 1 April 2019), p. 1012.

77 See Mike Carter, "Investigation of FBI's Child Pornography Operation Sparks Controversy Over Internet Privacy" (Government Technology, August 31, 2016).

78 See James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" [website] (FBI, 16 October 2014). Available at: www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed: 21 October 2021).

79 See Federal Parliament of Germany, Act to Make Criminal Proceedings More Effective and Practicable, 17 August 2017, BUNDESGESETZBLATT (BGBl.] [Federal Law Gazette] I at 3202, (amendments to 100a and 100b Code of Criminal Procedure).

80 See GRETA, *Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Germany* (20 June 2019). Available at: www.rm.coe.int/greta-2019-07-fgr-deu-en/1680950011 (accessed 29 November 2021). See commentary on s100a and b.

81 See Simmons + Simmons, "Pioneering Dutch Computer Crime Act III entered into force" [website] (Simmons + Simmons, 1 March 2019). Available at: www.simmons-simmons.com/en/publications/ck0bi70lg7kew0b94qi4inld1/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force (accessed 21 October 2021).

82 See Royal Decree of September 14, 1882 for the approval of the Criminal Procedure Law of Spain, Article 282, 4(c).

83 See Kristin Finklea, *Law Enforcement Using and Disclosing Technology Vulnerabilities* (Congressional Research Service, 26 April 2017), p.3.

84 In Ukraine in 2017–2018, amendments to the Commercial Procedural Code, to the Civil Procedure Code and to Administrative Procedure Code were adopted, and the ISO IEC 27037: 2017 standard "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence" was implemented. For example, draft law No. 4004 "On Amendments to the Criminal Procedure Code of Ukraine to increase the effectiveness of response against cybercrime and the use of electronic evidence" was submitted to the Verkhovna Rada of Ukraine on 1 September 2020. It provides for introduction of the institution of electronic evidence as information in electronic (digital) form with data that can be used as evidence of fact or circumstances that are established during criminal proceedings.

The use of e-evidence in court can also prove challenging – for example, in Montenegro there is no clear detailed regulatory framework for obtaining, searching or handling digital evidence, which lies at the heart of many successful prosecutions for technology-facilitated THB offences.[85] Even more challenging, in Kazakhstan as of 2019, evidence of recruitment of THB victims via social media platforms and messaging apps could not be used in criminal cases. This has led to recruiters – who may operate separately from those conducting the exploitation itself – often evading prosecution.[86]

d. Evidence generated through artificial intelligence

Another emerging topic in the area of e-evidence is the generation of evidence in THB cases with the use of artificial intelligence (AI) tools where the human factor is minimal or absent in general. Examples of e-evidence in THB cases generated by software without human intervention already exist. A number of projects in the United States, including those managed by law enforcement, are using chatbots to engage with sex buyers attempting to procure "services" of THB victims. The correspondence between the chatbots and buyers provides evidence of the criminal intent of the buyers and could be used in courts by prosecutors. Although this practice is already used in some OSCE participating States, it is not clear how policymakers and magistrates in the OSCE region will treat evidence gathered by an AI system. There is thus a need for clear and balanced policies and laws in this field.

85 Written contribution by the competent authorities of Montenegro, 06 October 2020.

86 See Mayya M. Rusakova, *Study Report. Exploring the Role of ICTs in Recruitment for Human Trafficking in the Republic of Kazakhstan, the Kyrgyz Republic and the Republic of Tajikistan* (International Organization for Migration, 2019), p. 22.

PART C Policy approaches to online platforms

1. Introduction

The central conversation in this paper is whether and how technology companies should be regulated as part of the global response to THB. The scope and scale of the role played by online platforms in illicit activity has heightened attention on this discussion and fuelled debate regarding the role of such online platforms in preventing and disrupting these illicit markets, including THB. A number of multilateral bodies, including the OSCE and the Council of Europe, have stressed the pivotal role played by private technology companies in providing services which are misused to commit illicit activities online, and identified the need to more specifically address the intersection of ICT and THB.[87]

There are several threshold considerations for policy makers. First and foremost is the degree to which the operations and practices of the technology sector should be self-regulated, co-regulated or government-regulated. Second, and closely related to the self-regulation - government regulation debate, is whether compliance with industry standards should be voluntary or mandatory.

As will be discussed below, the dominant model of regulation since the internet became public has been self-regulation and voluntary compliance. The combination of these principles has led to promising examples of innovation, unilateral action and co-operation. But it has also been characterized by fragmented, inconsistent and ineffective responses to the misuse of technology, with company efforts ranging from inspiring commitment to passive engagement to no action at all. In response to the growing misuse of technology, widely publicized harms and fragmented responses, there is a growing call to replace or supplement self-regulation with more assertive State-led policies.

A third major area of discussion, which is reflected in this part but also discussed in Part D, is defining the appropriate relationship between combating exploitation and fostering safety online, and upholding other objectives, rights or principles such as privacy, data protection, free speech, innovation and economic development. At times, these conversations have been presented as binary, competing debates (e.g., safety vs. privacy), but the reality is more nuanced. For example, whether privacy is at odds with safety depends on the definition of privacy and whose privacy is at issue – safety measures could be, for example, entirely consistent with protecting the privacy rights of sexually abused children whose images are shared online.

There is no consensus on any of these issues. Notably, there is not even consensus on a single definition of online platforms, reflecting the challenges of accurately defining a term that comprises a vast and dynamic range of services, functions and business models.[88] While recognizing the wide range of online platforms, this report adopts the definition proposed by the OECD, namely "digital service[s] that facilitate interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet". The analysis below examines these principles, including their successes and failures in practice, with a view to supporting more informed policy making across the OSCE region.

2. Self-regulation and co-operative approaches

Co-ordinated, State-led policy responses to technology-facilitated THB at the national and international level are very limited. In many cases, the lack of State policies and regulations has been intentional because – in most of the OSCE region – self-regulation has long been the predominant form of governance of online platforms. Indeed, some regional entities, such as the European Commission, have actively touted self-regulation as an impor-

87 See Council of Europe, Internet Governance - Council of Europe Strategy 2016-2019 (Council of Europe, September 2016), p. 10.

88 See European Commission, Commission Staff Working Document. Online Platforms Accompanying the document Communication on Online Platforms and the Digital Single Market. SWD(2016) 172 final (Brussels, European Commission, 25 May 2016), p. 2.

See OECD, An Introduction to Online Platforms and their Role in the Digital Transformation (OECD, 13 May 2019), p. 20.

See also Bertin Martens, An Economic Policy Perspective on Online Platforms. Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05 (European Commission, 2016), p. 3.

tant (and in some cases primary) element of online platform regulation.[89] "Self-regulation" should be understood as the "possibility for economic operators, the social partners, non-governmental organizations or associations to adopt among themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)."[90] A common feature of self-regulation initiatives has been the adoption of such common guidelines on a voluntary basis.

Self-regulation has also been encouraged by international instruments, such as the Lanzarote Convention, which "encourages the private sector, in particular the information and communication technology sector, the tourism and travel industry and the banking and finance sectors, as well as civil society, to participate in the elaboration and implementation of policies to prevent sexual exploitation and sexual abuse of children and to implement internal norms through self-regulation or co-regulation."[91] Articles 11 to 13 describe in detail what mechanisms are needed for the effective support of underage victims. Article 12 suggests development of hotlines for reporting of illegal material, while Article 13 suggests development of anonymous helplines (internet or phone) in all Member States for children and their parents or caretakers, allowing users to call in anonymously to seek advice.[92]

In light of the historical reliance on self-regulatory approaches (and the relative lack of State policies and regulations to address technology-facilitated THB), it is important to consider how the technology sector has responded in practice, what good practices have been developed, and what partnerships are being established that could be replicated at the national/regional levels through State policies.

There are various self-regulation forms, tools and initiatives. Two illustrative examples – Terms of Use and harmonization of industry standards – are discussed below.

a. Terms of Use

Terms of Use – which can have different titles depending on the service provider, such as Terms and Conditions, Terms of Service, Community Guidelines, etc. – adopted by online platforms constitute a foundational part of "self-regulation".[93] Principally, Terms of Use constitute a mechanism for a technology company to discourage and prevent certain activity on its platform, obtain consent to monitor and remove content on the platform, and sanction or remove users who violate the conditions.

Online platforms have responded to growing public critique of widespread misuse of their services by making these Terms of Use increasingly stringent. For example, Microsoft updated their services agreement to include the termination of services if users are found to share or publicly display "inappropriate content or material (involving, for example, nudity, bestiality, pornography, offensive language, graphic violence, or criminal activity)".[94] The new agreement went into effect in May 2018 [95] and applies to several of Microsoft's offered services, including Office, Skype, Bing and Xbox Live.

Although Microsoft did not specifically define what constitutes 'offensive language' in the agreement itself, or how they planned to evaluate what is offensive, the Microsoft Services Agreement includes a Code of Conduct that outlines what is allowed and what is prohibited when using a Microsoft account. Offensive language is cited as an example of inappropriate content or material. The company further included in the service agreement that it reserves 'the right to review' user's content in order to 'resolve the issue'.[96]

A number of social media companies, including some of the largest like Facebook, VKontakte and Youtube, commit more specifically in their Terms of Use to removing content that "facilitates or coordinates the exploitation of humans, including human trafficking."[97]

89 See European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe {SWD(2016) 172 final} (Brussels, European Commission, 25 May 2016), p. 9.

See also C. Parker, "Meta-Regulation: Legal Accountability for Corporate Social Responsibility". In: D. McBarnet, A. Voiculescu, T. Campbell (eds.), The New Corporate Accountability, pp. 207–237 (Cambridge University Press, 2007).

90 See European Parliament, Council and the Commission, Inter-institutional Agreement on Better Lawmaking, OJ C 321/01. (Official Journal of the European Union, 2003), p. 22.

See OSCE, "Statement by Petya Nestorova, Executive Secretary of the Council of Europe Convention on Action against Trafficking in Human Beings", 19th Alliance against Trafficking in Persons: Panel 4 [website] (Vienna: OSCE, 18 April 2019), starting from 32:57. Available at: www.osce.org/cthb/420167 (accessed 21 October 2021).

91 See Council of Europe, Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote, 25 October 2007), art. 9, p. 2.

92 See Global Initiative Against Transnational Organized Crime, Preventing Vulnerability of and Strengthening Policy Responses For Commercial Sexual Exploitation Of Children In The Western Balkans (working title) – forthcoming.

93 See Paul-Jasper Dittrich, *Online Platforms and How To Regulate Them: An EU Overview*, Policy Paper No.227 (Berlin, Jacques Delors Institut, 14 June 2018), p. 7.

94 See Microsoft, Microsoft Services Agreement. Available at: www.microsoft.com/en-us/servicesagreement/default.aspx (accessed 21 October 2021).

95 See Eric Limer, "Microsoft to ban "offensive language" from Skype" [website] (Popular Mechanics, 26 March 2018). Available at: www.popularmechanics.com/technology/apps/a19597085/microsoft-service-agreement-offensive-language/ (accessed 21 October 2021).

96 See Microsoft, Microsoft Services Agreement. Available at: www.microsoft.com/en-us/servicesagreement/default.aspx (accessed 21 October 2021).

97 See Facebook, Facebook Terms of Service. Available at: www.facebook.com/terms.php (accessed 21 October 2021).

Companies use the Terms of Use to take action against prohibited content. For example, Google was reported to have started blocking sexual content on its Google Drive platform in 2018. Google's action was in line with its updated Abuse Program Policies and Enforcement[98] which applied to its Drive, Docs, Sheets, Slides and new Sites. Under the "Sexually Explicit Material" section, the policies prohibit distributing "sexually explicit material, such as nudity, graphic sex acts, and pornographic material". A Google spokesperson stated that Google Drive enforced this with a combination of manual review and automated algorithms to evaluate violations.[99]

It is unclear whether companies view Terms of Use as a deterrent to certain conduct, or merely as a tool for obtaining consent and allowing the company to respond to violations. Given the volume of misuse online, including mainstream websites and social media platforms, however, it seems clear that Terms of Use are not broadly effective as a deterrent. This could also be explained by the fact that the majority of users of online service providers do not read Terms of Use and are not familiar with their content. One 2017 survey found that 91% of consumers willingly accept legal terms and conditions without reading them before installing apps, registering Wi-Fi hotspots, accepting updates or signing on to online services such as video streaming. For persons aged 18 to 34, the rate of acceptance of terms and conditions without reading them is as high as 97%.[100]

Acknowledging that diversity in the Terms of Use allows online platforms to build different types of communities in line with different purposes or business models, it also must be highlighted that without an industry standard on Terms of Use and their enforcement, especially regarding illegal activities and content, each company's approach will differ, resulting in uncertainty on all sides about what conduct is allowed and what is prohibited. Potentially, this can create safe havens for criminal actors.

b. Efforts to harmonize industry standards within the framework of self-regulation and multi-stakeholder initiatives

Several initiatives have attempted to improve self-regulation by harmonizing responses across the technology industry. Such efforts might involve exclusively the private sector, the private sector together with civil society, or multi-stakeholder groups that also include governments. Civil society organizations have been particularly active in trying to mitigate the negative consequences of the self-regulation principle by mobilizing efforts between various stakeholders to advance policy dialogue on countering the misuse of technology for THB.[101]

A key approach that has been adopted by the private sector and civil society in their endeavour to foster certain policies and practices and promote action-driven change is to establish multi-stakeholder initiatives involving different types of organizations. By leveraging the influence and institutional reach of the involved organizations, this approach multiplies advocacy efforts to achieve greater impact.

For example, the Technology Coalition[102] works to facilitate the technology industry's fight against online CSE. Founded in 2006 and reignited in 2020 with the launch of Project Protect, the Technology Coalition is an alliance of technology companies that enables sharing of knowledge and technology used in the prevention, detection, reporting, and removal of child sex abuse materials online. The Technology Coalition aims to align those in the industry who are working to tackle online child sexual abuse, pools their knowledge, and facilitates the sharing of technology, while using the expertise of industry members to develop the guidance and practices that help new and smaller companies to ramp up their capacity to protect children on their platforms.

A good example of an attempt to harmonize industry standards is Project Protect by the Technology Coalition. Launched in June 2020, Project Protect is a plan of co-ordinated action to drive the technology industry's efforts to fight child sexual abuse and exploitation online. One of the latest activities within Project Protect is a new initiative to develop a voluntary industry framework for transparency reporting. The development of this framework would represent a step forward in the pursuit of greater industry transparency and accountability. It would also improve available data and give greater insight into action to address child sexual exploitation and abuse online.

A prominent multi-stakeholder initiative focusing on policy is the WeProtect Global Alliance,[103] founded

98 See Google, "Abuse Program Policies and Enforcement" [website] Available at: www.support.google.com/docs/answer/148505?hl=en (accessed 21 October 2021).

99 See Samantha Cole, "Sex Workers Say Porn on Google Drive Is Suddenly Disappearing" [website] (Vice, 21 March 2018). Available at: www.vice.com/en/article/9kgwnp/porn-on-google-drive-error (accessed 21 October 2021).

100 See Deloitte, *2017 Global Mobile Consumer Survey: US edition The dawn of the next era in mobile* (Deloitte, 2017), p. 12.

101 Traditionally, civil society has been active in the fight against THB by providing victim assistance, raising awareness on the issue of THB, or advocating for survivors' rights. However, in recent years, civil society has increasingly advocated concrete policies and legislation. This has involved establishing alliances with the private sector across different industries to bring a more holistic approach to addressing the risk of THB in globalized economies. This advocacy has extended to addressing technology-facilitated THB.

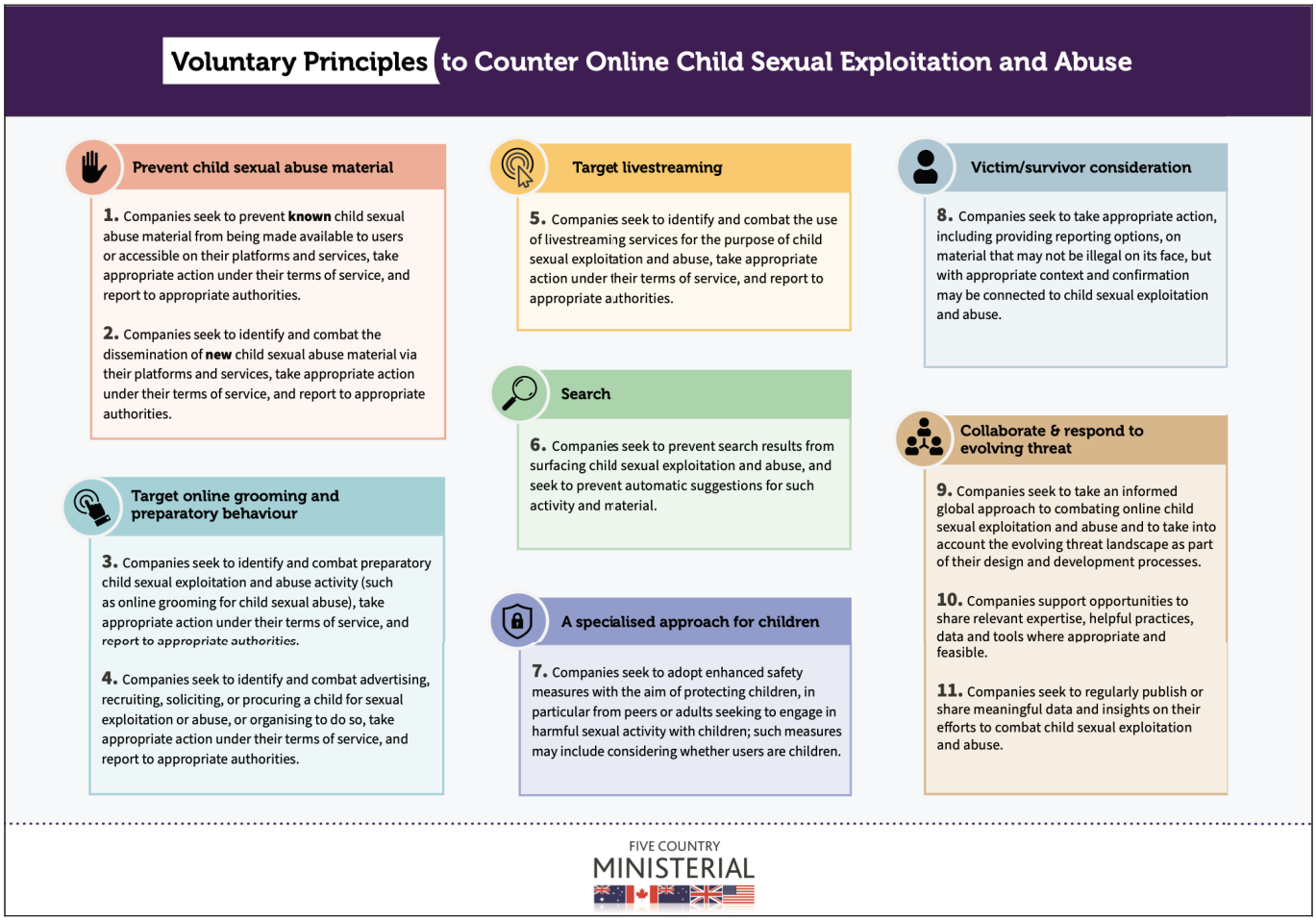
102 See The Technology Coalition [website]. Available at: www.technologycoalition.org/ (accessed 21 October 2021).

103 See WeProtect Global Alliance [website]. Available at: www.weprotect.org (accessed 21 October 2021).

in 2013 and led by the UK Government. Founded by Baroness Joanna Shields and supported by over 84 countries, 24 technology companies and 20 civil society organizations, WeProtect's mission is to stop the global crime of online child sexual abuse and exploitation. The initiative launched as an independent organization in 2020, and is now working to: ensure that senior decision makers take action on exploitation, including through empowering children and survivors; act as the definitive source of knowledge on the threat and response to exploitation-related crime through their "Model National Response" and organizing of "Hackathons"; and forge new networks to drive collaboration aimed at delivering a global response to online child sexual exploitation. The Alliance advocates for the adoption of global Voluntary Principles (see below for more on the Principles) to combat online child sexual exploitation.[104] It is also working to develop a range of products to support governments, industry and civil society to create a global strategic response to this type of exploitation and abuse.[105]

Initiatives such as the Technology Coalition and WeProtect are not traditional models of self-regulation such as Terms of Use; rather, these initiatives serve as co-operative mechanisms and spaces for collaboration among different stakeholders to facilitate a common approach to combating technology-facilitated human trafficking, especially for online sexual abuse of children. However, for the purpose of this report they are included in the self-regulation section since at the core of these initiatives is an intent to address technology-facilitated THB in a co-ordinated fashion based on their own decisions and assessment, rather than at the direction of a state-adopted policy.

Collaborative efforts between the private sector, government agencies and civil society organizations on the policy front have also resulted in the development of industry-led enforcement projects, such as the 2012 Operation Game Over, where "Microsoft, Apple, Blizzard Entertainment, Electronic Arts, Disney Interactive Media Group, Warner Brothers and Sony" took down "more than 3,500 accounts of New York registered sex offenders" from online video game platforms (e.g., Xbox Live and PlayStation),[106] although the legislation in place at that time did not impose such obligations on a number of the stakeholders.



104 See Five Countries Ministerial, *Voluntary Principles to Counter Online Child Sexual Exploitation* [website] (U.S. DOJ, 5 March 2020). Available at: www.justice.gov/opa/press-release/file/1256061/download (accessed 21 October 2021).

105 See WeProtect Global Alliance [website]. Available at: www.weprotect.org (accessed 21 October 2021).

106 See New York State Office of the Attorney General, "A.G. Schneiderman's "Operation: Game Over" Purges Thousands Of Sex Offenders From Online Video Game Networks" [website] (Office of the NY Attorney General, 5 April 2012). Available at: https://ag.ny.gov/press-release/2012/ag-schneidermans-operation-game-over-purges-thousands-sex-offenders-online-video (accessed 21 October 2021).

Private companies (e.g., Facebook, Google and others) have also worked together to create an industry hash sharing platform ("a cloud-based hash sharing tool") in order to harmonize take-down practices of child sexual exploitation and abuse material from online platforms.[107] The platform is integrated in the National Center for Missing and Exploited Children CyberTipline reporting system to facilitate and better organize the work of technology companies in this area. From a policy perspective, this initiative can also be considered as an effort to co-ordinate the industry-wide efforts to address online sexual exploitation of children.

On 5 March 2020 the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse was launched in Washington, D.C., a joint initiative of the Five Eyes countries (an alliance comprised of Australia, Canada, New Zealand, United Kingdom and United States), six major technology firms, and a broad range of experts from industry, civil society and academia. This initiative is an interesting one as it combines a policy approach taken by governments (namely voluntary compliance with an agreed set of principles) and by private sector companies (commitment to a set of principles of action) under a single umbrella. The Voluntary Principles cover issues ranging from online grooming and livestreaming of child sexual abuse, to industry transparency and reporting. Designed to be flexible so they can be implemented by any company (regardless of size or platform format), they provide a strong message for companies to address the scale and nature of the online child sexual abuse being facilitated on their platforms.[108]

The EU Alliance to Better Protect Minors Online also operates as a self-regulatory initiative designed to improve the online environment for children and young people. The initiative is aimed at tackling some of the emerging risks faced by minors online, including harmful content and conduct. The Alliance is partnered by 28 leading ICT and media companies, as well as by 14 NGOs and other stakeholders. All members are committed to the Alliance's three main strands of work: internet user empowerment; enhanced collaboration with various organizations and technology companies; and raising awareness of issues related to child online safety, digital empowerment and media literacy. It has produced an independent report detailing how the Alliance is being implemented, its impact, and the relevance and effectiveness of its actions since its launch in 2017. The report is a resource for learning from success stories and identified good practices.[109]

c. Limits of self-regulation and voluntary approaches, and the shift toward State-led action

As noted above, there are a number of examples of technology companies that have voluntarily undertaken significant efforts to prevent and combat exploitation and THB. These efforts have in some cases resulted in enhanced corporate policies and collaborative approaches. Thus, it is important for governments and the anti-trafficking community to recognize that the technology sector has not always been uniformly passive or merely reactive regarding misuse of their platforms for THB purposes. Indeed, some corporate policy initiatives and projects have had a crucial impact in addressing the online exploitation of people. The technology sector has also offered innovative online tools. And finally, initiatives from the private sector - and multi-stakeholder groups - can often offer valuable lessons for developing State-led initiatives.

Nonetheless, recent history suggests there are many shortcomings in self-regulatory approaches. The power of platforms to self-regulate according to different rules creates a fragmented regulatory landscape. It also provides no guarantee that content facilitating THB is included in industry standards, both in cross-industry initiatives and in individual Terms of Use. Further, platforms may lack incentives to report technology-facilitated trafficking to the public and authorities on their services given the risks of reputational damage and follow-up action being taken.[110] For example, media sources have reported on cases when online platforms did not fully disclose information regarding their platforms being used for trafficking purposes in order to avoid reputational risks.[111]

Self-regulation is also undermined by broadly worded rules or standards lacking in clear indicators of compliance or breach. Some companies suggest

107 See UNODC, "E4J University Module Series: Cybercrime, Module 12: Interpersonal Cybercrime. Online child sexual exploitation and abuse" [website] (UNODC, February 2020). Available at: www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html (accessed 21 October 2021).

108 See Five Countries Ministerial, *Voluntary Principles to Counter Online Child Sexual Exploitation* [website] (U.S. DOJ, 5 March 2020). Available at: www.justice.gov/opa/press-release/file/1256061/download (accessed 21 October 2021).

109 See European Commission, "Alliance to better protect minors online" [website]. Available at: www.digital-strategy.ec.europa.eu/en/policies/protect-minors-online (accessed 21 October 2021).

110 See Mark Dunn, "Reputational risks are greater than ever for brands associated with slavery" [website] (LexisNexis, 8 October 2019). Available at: www.bis.lexisnexis.co.uk/blog/categories/governance-risk-and-compliance/risks-greater-than-ever-brands-associated-with-slavery (accessed 21 October 2021).

111 See Justin Scheck, Newley Purnell and Jeff Horwitz, "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show." [website] (WSJ, 16 September 2021). Available at: www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953?mod=article_inline (accessed 25 January 2021).

that initiatives may need such broad wording to allow for a range of services of very different types and capabilities to implement measures appropriate to their service. However, while this position reasonably highlights potential negative consequences of specificity, the additional lack of enforcement mechanisms in self-regulation approaches means that broad wording is often interpreted in favour of business interests rather than safety.

Important questions about the efficacy of self-regulation measures have also been raised. Despite widespread and strongly worded prohibitions in Terms of Use regarding the misuse of online platforms for facilitating THB offences, misuse of ICT is rampant and accelerating. The misuse of online platforms continues to offer new business "opportunities" to traffickers, the ability to livestream sexual exploitation for instance has hugely increased the client base as well as the profitability of THB crimes.[112] Reports of online child sexual abuse and exploitation received by the NCMEC grew twenty-fold between 2013 and 2020, from 1 million to 21.4 million.[113] This indicates that while Terms of Use might be useful to empower a company to remove content or a user, they are not effective as a deterrent to motivated bad actors. More effective prevention mechanisms are needed.

Self-regulatory approaches have also allowed major gaps or blind spots in the global response to fester. For example, initiatives such as the WeProtect Global Alliance have shown promise in preventing technology-facilitated exploitation. However, the main focus of these efforts is on children; they do not address the exploitation of adults, despite the fact that adults represent the majority of identified trafficking victims. Indeed, sexually exploited adults are rarely part of the regulatory conversation; the OSCE is unaware of any similar initiatives focused on combating technology-facilitated trafficking of adults.

Contributing to these challenges is the fact that not all technology companies have the same resources or the same level of maturity; tech start-ups often have less systems in place, lack experience regarding the misuse of their platforms, or do not have developer capacity to respond to myriad safety issues. While larger companies might assertively pursue the implementation of safety measures using a self-regulatory model, smaller companies often prioritize other business decisions and defer such measures.

Moreover, the size of a tech company may not be the most critical factor. While companies with a focus on corporate responsibility or those that are concerned about their public reputation might be incentivized to adopt or comply with voluntary principles, companies operating in sectors with the greatest risks of exploitation (such as commercialized sexual services) may not be inclined to introduce voluntary measures that could harm business. Some stakeholders also note that technology companies are "terrifyingly slow in responding to the societal challenges they have created" – namely, online platforms that are misused to facilitate all elements of THB offences, from recruitment to exploitation.[114]

In light of these deficiencies, it is clear that the response to the misuse of online platforms cannot be underpinned by self-regulation alone. States, and indeed all actors beyond the online platforms themselves, are powerless to enforce self-regulation.[115] There is growing recognition that State-wielded standards, sanctions and enforcement powers are a necessary complement to self-regulation.

Petya Nestorova, the Executive Secretary of the Council of Europe Convention on Action against Trafficking in Human Beings, captured this need succinctly, stating that "self-regulation is inefficient by itself, as there is little oversight over enforcement of self-commitments and insufficient predictability". She called for "clear regulatory frameworks … where States do not 'oblige platforms to co-operate voluntarily', but set clear boundaries."[116] Similarly, the UK Government "Online Harms White Paper", which outlines a new regulatory approach for online platforms, states that its new framework "mov[es] far beyond self-regulation," implicitly recognizing the limitations of this approach.[117]

The call for increased State involvement in regulating online entities is consistent with the relatively recent trend observed in regulating the offline private sector with regard to human rights abuses. Until 2010, non-binding frameworks, such as the OECD Guidance on Practical Actions for Companies to Identify and Address the Worst Forms of Child Labour in Mineral Supply Chains, were the preferred approach

112 See OSCE and Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools* (Vienna: OSCE and TAT, May 2020), p. 12.

113 See NCMEC, *2020 Reports by Electronic Service Providers (ESPs)* [website]. Available at: www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf (accessed 21 October 2021).

114 See OSCE, "Statement by Halla Gunnarsdóttir, Special Adviser on Gender Equality, Iceland, 19th Alliance against Trafficking in Persons: Panel 4" [website] (Vienna: OSCE, 18 April 2019). Available at: www.osce.org/cthb/420167 (accessed 21 October 2021), starting from 48:30.

115 See Lucia Bird Ruiz-Benitez de Lugo, *Battling Human Trafficking, A Scrutiny of Private Sector Obligations under the Modern Slavery Act* (Geneva, The Global Initiative against Transnational Organized Crime, April 2018), p. 13.

116 See OSCE, "Statement by Petya Nestorova, Executive Secretary of the Council of Europe Convention on Action against Trafficking in Human Beings", 19th Alliance against Trafficking in Persons: Panel 4 [website] (Vienna: OSCE, 18 April 2019). Available at: www.osce.org/cthb/420167 (accessed 21 October 2021), starting from 32:57.

117 See UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper* (UK Government, 8 April 2019), p. 3.

to enhance private sector engagement.[118] In the last decade, however, the widespread recognition that the non-binding aspects of such codes significantly hamper their effectiveness has led to a global trend in legislation designed to fight human rights violations in supply chains.[119]

Similarly, despite resistance in some parts of the private sector, there is a growing push in the area of technology-facilitated trafficking to move away from regulatory approaches based solely on self-regulation and toward State-led frameworks, including ones that combine self-regulation of online platforms with enhanced State powers and oversight.[120]

3. Current developments in State-led regulatory approaches

Across the OSCE region, there are multiple efforts underway aimed at increasing State-led regulation in the area of technology-facilitated THB and exploitation. Two current examples that give insight into the evolving approaches, as well as introduce a number of specific topics covered in the following sections of the paper, are in the EU and the United Kingdom.

a. The EU Digital Services Act

Regulatory reform at the EU level is actively underway and the outcome could trigger a wider re-evaluation of governance frameworks regulating online platforms. In December 2020, the European Commission published the proposed Digital Services Act (DSA), which will update the existing E-Commerce Directive.[121] The proposed DSA does not fundamentally alter the EU's position on two core principles: 1) no general duty for companies to monitor third-party content, and 2) no liability for third-party content. However, it does outline a raft of additional obligations for online platforms, and shifts the balance towards mandatory – rather than voluntary – compliance. These obligations include enhanced requirements for addressing notifications of allegedly unlawful content, far-reaching transparency obligations (including the publication of detailed reports regarding the handling of unlawful content), and obligations to report to law enforcement authorities "any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place." (These concepts of notice and take down, transparency and reporting are discussed further in sections below.)

Breach of obligations under the DSA would be penalized by hefty fines of up to 6% of annual income, or turnover of the online provider. Intermediaries without EU establishments would be required to designate legal representatives in the EU, in part to facilitate enforcement. Notably, the EU Commission will have supervisory and enforcement powers over platforms with over 45 million active monthly users (designated as "very large" platforms).[122]

In addition to the above, "very large" platforms would be required to identify and analyse "significant systemic risks" arising from their services, including their role in illicit markets, and then take "proportionate" steps to mitigate these risks. Moreover, the obligation for "very large" platforms to share data with researchers could be of significant value, including informing the improvement of regulation going forward. While it remains to be seen what these obligations would look like in practice, they could herald significantly enhanced duties to mitigate the use of online platforms in the context of THB marketplaces.

These steps demonstrate the growing resolve to regulate online marketplaces, at least regionally, if not globally. At the same time, industry bodies have been extensively lobbying to ensure that the EU DSA will protect members' interests. In particular, the EU Tech Alliance has argued for maintaining the current

118 See OECD, *Practical Actions for Companies to Identify and Address the Worst Forms of Child Labour in the Minerals Supply Chains* (Geneva: OECD, 2017).

119 See Lucia Bird Ruiz-Benitez de Lugo, *Battling Human Trafficking, A Scrutiny of Private Sector Obligations under the Modern Slavery Act* (Geneva, The Global Initiative against Transnational Organized Crime, April 2018), p. 3.

120 See Christopher Marsden, *Internet Co-Regulation* (Cambridge University Press 2011), p. 46.

See also Michèle Finck, Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy (*European Law Review,* 20 June 2017). LSE Legal Studies Working Paper No. 15/2017. Available at: www.ssrn.com/abstract=2990043 and www.dx.doi.org/10.2139/ssrn.2990043 (accessed 29 November 2021).

121 Prior to publication of the proposal, the EU stated that the DSA would set out new illegal content liability rules for digital platforms, although introductory documents struck a cautious note in stating that the proposals will "respect the basic principles underpinning the current legal framework of the e-Commerce Directive." This echoed recommendations by European parliamentary committees, which demonstrated a preference for retaining the existing safe harbour, while in parallel strengthening mechanisms for holding platforms to account, and establishing legally binding take-down mechanisms. The Committee on Legal Affairs' legislative report (22 April 2020) focuses on ways the DSA can increase regulatory oversight of large platforms. It recommends establishing clear content moderation procedures and a "notice and action" framework, with any final decision regarding legality of content being made by a judicial rather than a private body. See: www.europarl.europa.eu/doceo/document/JURI-PR-650529_EN.pdf (accessed 27 November 2021). The Committee on the Internal Market and Consumer Protection's legislative report (24 April 2020) favours retaining the existing liability framework, whilst also proposing a legally binding take-down mechanism with recourse to an out-of-court dispute settlement and clarification regarding "active" and "passive" hosting. See: www.europarl.europa.eu/doceo/document/IMCO-PR-648474_EN.pdf (accessed 27 November 2021). The Committee on Civil Liberties, Justice and Home Affairs' report on fundamental rights issues posed by the DSA called for the creation of a new EU regulator which would have the power to impose sanctions based on a platform's transparency and how much it "amplifies" illegal content. The Committee on Civil Liberties, Justice and Home Affairs' own-initiative report on fundamental rights issues posed by the DSA (27 April 2020), available at: www.europarl.europa.eu/doceo/document/LIBE-PR-650509_EN.pdf (accessed 27 November 2021).

122 See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC* (Official Journal of the European Union, 15 December 2020), art. 54.

regime, with individuals rather than platforms continuing to bear the most liability.[123]

Nonetheless, there are still a number of unanswered questions regarding the scope of application of the current draft. The draft states that the DSA applies to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorized use of copyright protected material, or activities involving infringements of consumer protection law. But the definition of "illegal content" in the current draft of the DSA does not expressly include content related to THB activities, including exploitation of adults, which would be a glaring omission in the effort to protect vulnerable populations.

The DSA has been flagged by the European Commission as a key step in enhancing the rights of individuals to demand the removal of content, including across borders.[124] Additionally, the proposed DSA provides that the European Commission engages with the private sector and civil society to draw up codes of conduct setting out "harmonised European [due diligence] standards" for online platforms, although it is unclear whether these would be voluntary or binding.[125]

The proposed DSA remains in draft form, and discussions by the European Council to find a common position are ongoing. However, it signals the EU's proposed approach: preserving the status quo on liability and monitoring obligations, while simultaneously expanding the obligations of online platforms.

b. The UK Online Harms Bill

In 2019, the United Kingdom - which has made clear it will not implement the DSA - published the "Online Harms White Paper". This established a preliminary framework for the draft Online Safety Bill, which was published in May 2021. In the White Paper, the UK Government stated that the pending regulatory framework would "usher in a new age of accountability for tech companies".[126]

The re-think of online platform governance has been triggered by the sense that "progress has been too slow and inconsistent" by online platforms in mitigating the risk that their services are misused to commit criminal offences and propagate harm.[127]

Government rhetoric regarding the policy has repeatedly emphasized that the United Kingdom is seeking to pioneer a global standard for regulating digital services.[128] While the regulation of online platforms is under scrutiny across a range of jurisdictions, including the EU (as outlined above) and India, the position papers published by the UK Government to date point to particularly far-reaching change.

The bill, if implemented as currently drafted, would impose a new statutory duty of care on companies falling within its scope to "take action to prevent user-generated content or activity on their services causing significant … harm to individuals".[129] Companies will be required to implement systems to fulfil their duty of care[130] and an independent regulator – Ofcom (the current communications regulator) – will be granted significant powers to sanction breaches of the duty of care. These include fines of up to the greater of £18 million or 10% of annual turnover, and the power to block access to the services in the United Kingdom. The UK Government has also stated that it may introduce criminal sanctions for senior employees for failing to comply with Ofcom requests for information. While the Bill is not expected to introduce new avenues for individuals to sue tech companies, the government expects that "legal action will become more accessible to users as the evidence base around online harms grows."[131]

Although the UK Government has stated that the new framework will "increase the responsibility of online services in a way that is compatible with the EU's e-Commerce Directive['s]" position on liability, the policy papers triggered extensive lobbying by industry, which perceived the framework to impose

123 See European Tech Alliance, *European Tech Alliance Position on the future eCommerce framework ('Digital Services Act')*, (European Tech Alliance, April 2020), p. 1.

124 See Leonie Cater, "How Europe's privacy laws are failing victims of sexual abuse" [website] (Politico, 13 January 2021). Available at: www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/ (accessed 21 October 2021).

125 See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC* (Official Journal of the European Union, 15 December 2020), art. 34.

126 See UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper* (UK Government, 8 April 2019), p. 46.

See also UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper: Full Government Response to the consultation* (UK Government, December 2020), p. 3.

127 See UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper* (UK Government, 8 April 2019), p. 3.

128 Ibid, p. 7.

129 The new regulatory framework will apply to all companies whose services host user-generated content or facilitate interaction between users, one or more of whom is based in the United Kingdom. This includes encrypted messaging services and closed groups on social media platforms. There are a number of exemptions, including for business-to-business services, and low-risk businesses with limited functionality.

130 The UK Government responded to concerns raised during the consultation on the White Paper about the potential impacts on free speech by focusing on the systems companies have in place to address harmful content, instead of on the removal of specific content itself.

131 See UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper: Full Government Response to the consultation* (UK Government, December 2020), p. 27.

higher liability risks and more stringent obligations on tech companies.[132] These additional obligations include those targeted at enhancing transparency, discussed further below.

The White Paper also sets out an initial list of "harms" falling within the scope of the regulatory framework. These include child sexual exploitation and abuse, as well as modern slavery (which encompasses both THB for sexual exploitation and forced labour).[133] The draft Bill defines content that "is harmful to adults" broadly as that which is illegal, identified in supporting regulations, or which the "service provider would have reasonable grounds to believe" there is a "material risk" that the content would have "a significant adverse physical or psychological impact on an adult of ordinary sensibilities".[134] "Priority" forms of harmful content will be designated in supporting regulations. It remains to be seen whether these reflect those originally proposed by the White Paper.[135]

The Bill's potential role in addressing the misuses of online platforms for the facilitation of adult trafficking offences is being closely scrutinized by anti-trafficking stakeholders. The available sanctions could incentivize additional focus on preventing the misuse of online platforms to recruit and exploit victims of THB; notably, the power to block access to online platforms could be a powerful tool in acting against adult services websites which are widely misused by traffickers to advertise victims of THB for sexual exploitation. The Modern Slavery and Human Trafficking Unit of the UK's National Crime Agency has been actively engaging with the Home Office in the context of the legislation, including considering whether websites, specifically adult services websites, would have responsibilities to proactively look for indications of modern slavery and THB.[136]

132 See Madhumita Murgia and Martin Coulter, "Big Tech attacks UK plan to hold firms liable for harmful content" [website] (*Financial Times*, 1 July 2019). Available at: www.ft.com/content/3de70dd4-99ba-11e9-8cfb-30c211dcd229 (accessed 21 October 2021).

See also UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper: Full Government Response to the consultation* (UK Government, December 2020), p. 46.

133 See UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper: Full Government Response to the consultation* (UK Government, December 2020), p. 31.

134 See UK Parliament, *Draft Online Safety Bill*, article 46.

135 Ibid.

136 Telephone interview with Jessica Harrison, Operations Manager, Modern Slavery and Human Trafficking Unit, 19 November 2020.

PART D Specific Topics Related to Trafficking in Human Beings

As Part C outlined, the historical reliance on self-regulation appears to be shifting toward support for State-led regulatory approaches. Recent policy developments, including those related to the UK Online Harms Bill and the EU Digital Services Act, indicate that the catalyst for this shift is increased acknowledgment of the shortcomings of the self-regulatory approach, in particular the failure to stem exploitation and trafficking online.

If policy makers wish to avoid the deficiencies of the previous approaches, there are a number of key points of intervention related to technology-facilitated THB that require attention in law and policy. Within the framework of State-led regulation based on mandatory compliance, the core topics policy makers will need to tackle include prevention, monitoring, removal of prohibited content, liability, and transparency related to company actions.

1. Prevention

One area of focus for both the private and public sector on the topic of technology-facilitated THB has been the adoption and implementation of prevention measures by technology companies. It is important to note that such prevention measures are not a replacement for other holistic measures to address a whole-of-society harm such as THB, but rather should come alongside other prevention efforts. As with other interventions discussed in this report, prevention measures could be self-initiated by the technology companies or undertaken in response to a push from the public sector. Likewise, they could be voluntary or mandatory. Below, two examples of prevention measures - safety by design, and age and consent verification – are discussed, as well as the use of government-issued guidance to advance such measures. Another prevention measure – Terms of Use – is addressed above at p. 25.

a. Safety by Design

The "safety by design" approach puts the well-being and security of the users of digital services at the center of technology products and services development. In the effort to maximize profits, companies might be incentivized to introduce fewer safety mechanisms for users during the development phase in exchange for attracting more users or increasing engagement and content sharing.

This approach does not constitute a legal violation in many jurisdictions, since the technology sector is typically not regulated. However, as noted throughout this report, traffickers have taken advantage of the lack of strong safety measures for exploitative purposes. In order to find a solution to this problem, some experts have proposed a safety-by-design framework to promote the need to put users' rights and interests at the forefront of the digital ecosystem.

Australia, which is an OSCE Partner for Co-operation, is an example where safety by design principles are well defined and explained. According to the Australian approach, the safety by design principles provide a benchmark for industries of all sizes and stages of maturity, and aim to provide guidance in incorporating, enhancing and assessing user safety considerations throughout the design, development and deployment phases of a typical service lifecycle. The principles firmly place user safety as a fundamental design principle that must be embedded in the development of technological innovations from the start.[137] An example of practical implementation of the safety by design principle is when companies install default features such as SafeSites and SafeSearch which deactivate default incognito modes and prevent minors from accessing sexually explicit websites or searching for sexually explicit content in search engines.

b. Age and Consent Verification

Two related forms of prevention receiving increased attention in recent years are age and consent verification. Age verification typically refers to the process of confirming the age (or at least adulthood) of a visitor to a website or the user of a platform such as social media. Crucially, however, it also refers to the age of persons depicted in uploaded material. Age verification – especially with regard to visitors to websites - has seen significant attention lately, particularly as concerns about children viewing adult-oriented websites (e.g. pornographic sites) have grown. Again, this is a topic that may be addressed on a voluntary basis from the technology sector, as well as through mandatory policies adopted by States.

137 See Australian Government eSafetyCommissioner, "*Safety by Design" [website]* (eSafetyCommissioner, 2019). Available at: www.esafety.gov.au/industry/safety-by-design (accessed 21 October 2021).

A predominant method of age verification on many websites has been unverified certifications of age, typically the click of a button confirming that the user is over 18 years old, or entering a birthdate on the screen to affirm that the visitor to the site is an adult. These simplistic methods are used by many services, including social media platforms and even pornographic websites, where the risks of harm to children are higher. Such mechanisms to verify age have been subject to the criticism that they are highly ineffective. For example, one recent study found that 27% of boys aged 9 to 12 report having used a dating app that supposedly should only be used by adults.[138] Recently, however, approaches have trended toward more robust and accurate age-verification. For example, the dating app Tinder introduced a significantly stronger age verification mechanism in Japan. The minimum age requirement for Tinder is 18 years old; Tinder members in Japan are asked to verify their age with a Japanese passport, driver's license or health ID to prove that they meet this requirement, in accordance with local law.[139]

The public sector has also increased engagement in this area. A number of countries have promoted laws and guidance aimed at the implementation of age verification for visitors to online platforms with the goal of preventing exploitation of minors. In the United Kingdom, the Children's Code[140] applies to UK-based companies and non-UK companies who process the personal data of UK children. It requests companies to voluntarily implement appropriate measures, such as mapping what personal data is collected from UK children; checking the age of people who visit websites, download apps or play games; switching off geo-location services that track where in the world visitors are; not using "nudge" techniques to encourage children to provide more personal data; and providing a high level of privacy by default.

In 2020, France introduced a nationwide age verification system for pornography websites as part of a broader law on domestic violence. The intent of the policy is to ensure that minors do not have access to pornographic content. In order to enforce the law, the French audio-visual regulator CSA will be granted new powers to audit and sanction companies that do not comply — sanctions could go as far as blocking access to the websites in France with a court order. The choice of verification mechanisms will be left up to the platforms.[141]

Germany is undertaking similar measures with regard to age verification, and appears to be enforcing the provisions. In the summer of 2021, German officials initiated action against four major pornography websites for failure to introduce age verification checks to stop persons under 18 from accessing pornography. The actions are undertaken to enforce an agreement of child protection, to which all German states have signed.[142]

Most of these initiatives are focused on verifying the age of visitors to websites to ensure, for example, that children are not viewing pornography. However, equally or even more important – but much less common – are measures to ensure that the content being uploaded or shared on these platforms does not feature minors, for example in child sexual abuse imagery or sexual service advertisements. In its report on Criminal Networks Involved in the Trafficking and Exploitation of Underage Victims in the EU, Europol concludes that "the online advertisement of sexual services is an increasing phenomenon relating to THB for sexual exploitation, with children being advertised as adults".[143] However, most efforts to screen for minors in uploaded content are limited to checking for previously confirmed images of exploited children and not new images that might, for example, involve a trafficked teenager. Moreover, these efforts are typically focused on exchange of child sexual abuse material (CSAM) on the dark web or in closed groups on social media, rather than monitoring sexual service websites where minors are often advertised. In short, age verification applied to uploaded content in addition to website visitors is necessary to prevent exploitation of children. (This topic is also considered in other sections of this report below such as Monitoring).

Historically, consent verification has received less attention than age verification. However, a series of highly publicized cases involving rape and sexual assault videos uploaded to pornographic websites have prompted a closer look from authorities and parliaments. For example, in 2021 in Canada, the "STOP Internet Exploitation (SISE) Act" sought to establish a criminal offense to distribute pornographic content without verifying that the depicted individual currently consents to that distribution. Although this

138 See Thorn and Benenson Strategy Group, *Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking. Findings from 2020 quantitative research among 9–17 year olds* (Thorn, May 20219), p. 17.

139 See Tinder, "Age verify to chat with matches" [website] (Tinder). Available at: www.help.tinder.com/hc/en-us/articles/360041821872-Age-verify-to-chat-with-matches (accessed 21 October 2021).

140 See ICO, "Introduction to the Age appropriate design code" [website]. Available at: www.ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ (accessed 21 October 2021).

141 See Elisa Braun and Laura Kayali, "France to introduce controversial age verification system for adult websites" [website] (Politico, 9 July 2020). Available at: www.politico.eu/article/france-to-introduce-controversial-age-verification-system-for-adult-pornography-websites/ (accessed 21 October 2021).

142 See Tony Baggett, "Germany is about to block one of the world's biggest porn sites" [website] (Wired, 14 July 2021). Available at: www.wired.co.uk/article/germany-porn-laws-age-checks (accessed 21 October 2021).

143 See Europol, *Criminal networks involved in the trafficking and exploitation of underage victims in the European Union* (The Hague: Europol, 18 October 2018), p. 7.

type of prevention measure is still nascent, consent verification could be an avenue to reduce the exploitation of trafficking victims on sexual service websites. The SISE Bill is an example of a growing desire to prescribe stronger prevention measures through legislation.

c. Government-issued guidance

While maintaining a foundation of self-regulation based on voluntary compliance, some countries have attempted to trigger enhanced industry action by issuing guidance and recommendations to the private sector to improve safety online.

For example, the UK government launched in 2019 a guidance framework for a Code of Practice for providers of online social media platforms[144] on appropriate actions they should take to prevent bullying, insulting, intimidating or humiliating behaviours on their sites.

Likewise, in June 2021, the French National Commission on Informatics and Liberty published eight recommendations to strengthen the protection of minors online. Some of these recommendations are addressed to online services providers, such as providing specific guarantees to protect the interests of the child, checking the child's age and the parents' consent while respecting their privacy or seeking parental consent for minors under 15.[145]

These initiatives share commonalities with some of the multi-stakeholder initiatives described above. However, a key difference is that the public-facing product is typically developed and owned by the government rather than a multi-stakeholder body. In this sense, they constitute an effort by governments to support and mobilize companies, while still adhering to the traditional principles of self-regulation and voluntary compliance.

2. Monitoring

Current regulatory approaches to governing online platforms predominantly employ an approach that is reactive in addressing illicit activities facilitated by online platforms. Although some prevention efforts are utilized, as discussed in the previous section, most interventions aim at identifying prohibited content (i.e. "monitoring") and then removing or blocking it.

Consistent with the traditional self-regulation and voluntary approaches used in most countries, monitoring of content on platforms has been guided by the bedrock principle that online platform companies have no obligation to monitor third-party content (i.e. content uploaded by users of a platform, such as pictures or emails or advertisements).[146] As is stated in the "Recommendation of the Committee of Ministers to the Council of Europe on the roles and responsibilities of online platforms": "State authorities should not directly or indirectly impose a general obligation on intermediaries to monitor content which they merely give access to, or which they transmit or store, be it by automated means or not."[147]

The exemption from monitoring obligations has been called into question by a series of jurisprudence.[148] One key judgement is a 2019 European Court of Justice ruling, specifically relating to Facebook, which concluded that although EU Member States cannot impose "general monitoring" obligations on online service providers (in line with the EU E-Commerce Directive), they can "apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities".[149]

This has potentially wide-ranging ramifications for the duties that can be imposed on online platforms in the context of THB (to the extent that the content is manifestly unlawful), and child sexual abuse material online.[150] Ongoing inconsistencies between EU case law and the approaches taken by individual Member States have highlighted uncertainties that require resolution and a more harmonized approach.[151]

a. Intersection between monitoring and liability

The principle of no obligation to monitor has often been linked with a second, equally fundamental principle - no liability for third-party content. Although

144 See UK Department for Digital, Culture, Media and Sport, "Statutory guidance. Code of Practice for providers of online social media platforms" [website] (UK Government, 12 April 2019). Available at: www.gov.uk/government/publications/code-of-practice-for-providers-of-online-social-media-platforms/code-of-practice-for-providers-of-online-social-media-platforms (accessed 21 October 2021).

145 See French National Commission on Informatics and Liberty, "The Digital Rights of Minors" [website] (CNIL, 09 June 2021). Available at: www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne (accessed 21 October 2021).

146 While the EU Commission Recommendation on tackling illegal content online requests online platforms to adopt proactive tools for detecting and removing illegal content, this is non-binding.

147 This principle sits uncomfortably with the obligations on all businesses to conduct appropriate due diligence to minimize the risk of human rights breaches resulting from their services, as set out in the UN Guiding Principles on Business and Human Rights.

148 See Giancarlo F. Frosio, *The Death of "No Monitoring Obligations": A Story of Untameable Monsters* (JIPITEC, 2017), p. 3.

149 See InfoCuria Case-law, *Eva Glawischnig-Piesczek vs. Facebook Ireland Limited, October 2019, Case C-18/18* (Court of Justice of the EU, October 2019). Available at: www.curia.europa.eu/juris/document/document.jsf?docid=218621&doclang=EN (accessed 21 October 2021).

150 See Carolyn E. Pepper, "Monitoring online content: the impact of Eva Glawischnig-Piesczek v Facebook Ireland Limited" [website] (ReedSmith, 12 November 2019). Available at: www.reedsmith.com/en/perspectives/2019/11/monitoring-online-content-the-impact-of-eva-glawischnig-piesczek-v-facebook (accessed 21 October 2021).

151 In particular, there seems to remain confusion between "a general duty of care" and "content monitoring obligations".

liability is further addressed in section 4 below (p. 46), it is relevant here because of its fluid relationship with the topic of monitoring. Again, the Council of Europe Recommendation is illustrative: "States should ensure, in law and in practice, that intermediaries are not held liable for third-party content which they merely give access to or which they transmit or store." However, this is caveated for instances where intermediaries do not "act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature."[152]

The principles related to monitoring and liability are often enshrined together in national legislation. For example, in the United States, section 230 of the Communications Decency Act of 1996 provides a liability shield from state and federal civil laws for online platforms that function purely as hosts of third-party generated content. Section 230 also provides immunity from civil liability for voluntary, good faith efforts to moderate (i.e. monitor and remove) content the companies determine to be obscene, violent, harassing or otherwise objectionable. However, recent legislative amendments clarified that such liability shields do not apply to cases of human trafficking or promoting prostitution (discussed further below, p.47).[153]

Similarly, in the EU, the E-Commerce Directive prohibits the imposition of a general duty for online platforms to monitor their content, and provides that if an online platform acts as a mere conduit for information, it cannot be liable for the information being transmitted.[154]

However, the relationship between the two principles as enshrined in the E-Commerce Directive is not always clear. For example, jurisprudence from the European Court of Justice states that the liability exemption in the E-Commerce Directive only applies to online platforms fulfilling a "neutral" role, "in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores."[155]

This has given rise to concerns that online platforms conducting proactive monitoring to determine the legality of uploaded content and block or remove it where appropriate could be considered "active" rather than "neutral", thereby losing the benefit of the liability shield (known as the "Good Samaritan paradox").[156] The European Commission sought to allay concerns by stating in its Communication issued in September 2017 that voluntary proactive monitoring did not mean that the online platform loses the benefit of the exemption.[157] However, in the absence of a Court of Justice judgment – or amendments to the Directive – clarifying this point, the lack of certainty on liability creates a potential risk that online platforms will be dis-incentivized from taking more proactive monitoring steps.

The long-accepted position on the inviolability of these two principles is currently being challenged on a number of fronts.[158] Critics of the protections the principles afford to online platforms argue that they were designed to enable the growth of the internet, and that they are no longer required in an age in which online platforms have profits exceeding the GDP of many States. They highlight that the principles and key legislation enshrining them, such as the E-Commerce Directive and Communications Decency Act, were adopted in a very different technology landscape, where Facebook and Youtube had not yet been founded.[159] In public discourse, there is a growing sense that the bedrock principle of no duty to monitor – coupled with no liability for third-party content – requires updating.

b. Tensions between monitoring and privacy

Companies often conduct monitoring through a combination of human moderation and technology-facilitated moderation. As was discussed in the section on crises and COVID above, the relative balance between human moderation and technology-facilitated moderation can vary depending on a number of factors and is not constant. However, whether it is human or technology-facilitated, monitoring third-party content on platforms inevitably raises issues of privacy.

152 See New Zealand Harmful Digital Communications Bill 2013 (2014 No 168-2), which provides a "safe harbour" for ISPs, but interestingly makes this contingent on ISPs providing an "easily accessible mechanism that enables" users to contact hosts to complain about specific content.

153 See US Congress, US Communications Decency Act, 47 U.S.C. §230.

154 The meaning of "mere conduit": does not initiate the transmission, does not select the recipient, and does not select or modify the information. Article 15 Electronic Communications Directive prohibits the imposition of general monitoring obligations; Article 14 provides the exemption from liability.

155 See Cases C236/08 to C238/08 Google France vs. Louis Vuitton EU:C:2010:159, para. 113. Further case law has also cast doubt on where an online platform becomes "active". For example, see: Case C-324/09 L'Oreal et al. vs. eBay EU:C:2011:474: In para. 116 the Court of Justice stated: "Where, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability"; Case C-484/14 Mc Fadden EU:C:2016:689, para. 62. These cases are further discussed in Van Eecke (2011), Husovec (2017), Nordemann (2018), Van Hoboken et al. (2018).

156 See European Parliamentary Research Service, *Liability of Online Platforms* (Brussels: European Parliament, February 2021), p. 81.

157 See EUR-Lex, *Communication of the Commission on Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms, COM (2017) 555* (Brussels: Publications Office of the European Union, 28 September 2017), p. 10.

158 For example, see Estonia s11 Information Society Service Act, which enshrines no obligation to monitor. Available at: www.riigiteataja.ee/en/eli/515012019001/consolide (accessed 21 October 2021).

159 These arguments were repeatedly cited by stakeholders interviewed for this research in favour of tightening regulation of online platforms.

For example, the use of technology tools to monitor content has sparked a fierce debate between protecting privacy and enabling use of the technology tools to combat online sexual exploitation and abuse of children. On one side of the debate are privacy advocates, who believe that the use of technology tools to combat technology-facilitated THB are too intrusive and infringe the right to privacy. On the other side, anti-trafficking and exploitation experts argue that technology tools do not violate the right to privacy and serve to prevent and combat exploitation of people, especially of children. Further, while it is generally recognized that automated tools do not entirely obviate the need for human moderation, they can considerably reduce the impact on human moderators from viewing such content.

Two recent examples of this debate in action are explored below: the halt in the EU on monitoring content for child exploitation material in early 2021, and the increasing use of encryption by technology companies.

– The EU Electronic Communications Code

The implementation of the EU Electronic Communications Code (ECC), which should have been transposed by all EU Member States by 20 December 2020, highlights how regulatory amendments can create obstacles for efforts to address technology-facilitated trafficking and exploitation.[160]

A range of tools currently used to detect online child sexual abuse material, including Microsoft PhotoDNA and Google CSAI Match, were deemed illegal under the ECC. The tools relating to images generally create a unique digital signature (known as a "hash") of an image that is, for example, confirmed to be CSAM. This hash is then compared against signatures (hashes) of other photos on the platform to find copies of the same or similar image so that they can be seized and removed. The tools focusing on videos generally use hash-matching to identify prohibited content (based on comparisons to previously identified illegal content), allowing companies to identify this type of content amid a high volume of non-prohibited video content.

The detection tools, used widely by companies around the world to generate the overwhelming majority of CSAM reports, rely on screening user's content in a manner prohibited by the ECC. Thus, when the ECC went into effect and the tools could not be used, some companies such as Facebook temporarily stopped using the detection tools in the EU. The impact of this was enormous – the US National Center for Missing and Exploited Children reported a 58% drop in reports of EU-related child sexual exploitation beginning December 21, 2020 when the new regulations went into effect.[161] The rate of reporting would have undoubtedly have fallen further if some companies, such as Microsoft and Google, had not continued to use these tools during the period prior to the adoption of the derogation.

After considerable backlash from the anti-trafficking and child protection communities, including NGOs and tech companies that criticized the decision to forbid the use of tech tools, the European Commission proposed a temporary derogation from the e-Privacy Directive until 2025, to enable service providers to continue using existing tools "to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services".[162] Despite the limited scope of the derogation, a group of MEPs on the European Parliament's Civil Liberties, Justice & Home Affairs (LIBE) Committee initially opposed the derogation in late 2020, citing data protection concerns. The derogation was eventually approved.[163] Had the derogation not been approved, organizations would have been unable to legally use these tools within Europe, significantly hampering their ability to detect CSAM on the continent that, in 2019, hosted 89% of known URLs containing CSAM.[164]

The EU is a trendsetter in matters of data protection and online regulation. Closing the door on the use of technology tools to identify child sexual abuse material in the EU would have had significant impacts on efforts to address online exploitation. The fact that the Code initially came into effect without a derogation and immediately impacted the volume of reports highlights the ongoing challenges in regulating online marketplaces.

160 See WeProtect Global Alliance, "European Electronic Communications Code briefing" [website] (WeProtect Global Alliance, 16 December 2020). Available at: https://www.weprotect.org/library/european-electronic-communications-code-briefing/ (accessed 21 October 2021).

161 See John F. Clark, "We Are in Danger of Losing the Global Battle for Child Safety" [website] (NCMEC: 17 November 2020). Available at: www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety (accessed 21 October 2021).

162 See European Commission, "Fighting child sexual abuse: Commission proposes interim legislation to enable communications services to continue detecting child sexual abuse online" [website] (European Commission, 10 September 2020). Available at: https://digital-strategy.ec.europa.eu/en/news/fighting-child-sexual-abuse-commission-proposes-interim-legislation-enable-communications-services (accessed 21 October 2021).

163 See European Parliament News, "Detecting online child sexual abuse requires strong safeguards" [website] (European Parliament, 7 December 2020). Available at: www.europarl.europa.eu/news/en/press-room/20201207IPR93202/detecting-online-child-sexual-abuse-requires-strong-safeguards (accessed 21 October 2021).

See also European Parliament, *REPORT on the Proposal for a Regulation of the European Parliament and of the Council on a Temporary Derogation from Certain Provisions of Directive 2002/58/EC of the European Parliament and of the Council as Regards as the Use of Technologies by Number-Independent Interpersonal Communications Service Providers for the Processing of Personal and Other Data for the Purpose of Combatting Child Sexual Abuse Online* (11 December 2020).

164 See Internet Watch Foundation, *Annual Report 2019* (IWF, 2019), p. 52

Further, there is lack of clarity as to whether newly developed tools would fall within scope of the derogation. Given that addressing exploitation is an area where technological innovation is both desired and developing rapidly, failure to account for new tools could be a key obstacle to service providers seeking to enhance their responses to CSAM. There are currently ongoing discussions to find a longer-term solution that would balance privacy concerns and the need to protect children from being exploited online.

The above-described case highlights that it is important that policymakers acknowledge that there is a close relationship between policies and laws that form the global response to online exploitation and the tools and approaches developed by companies. It was companies that developed the ground-breaking tool to hash pictures so that copies of illicit images could be identified and removed. This highlights the potential for companies to substantively contribute to combating exploitation. On the other hand, while the tool has been widely acknowledged as a success, it still has important limitations.

For example, it is dependent on a database of previously known and confirmed illegal images; new, exploitative images are not identified by the software, but must be entered into the database by authorities. Second, there is currently no framework to identify, store and categorize content in cases related to the exploitation of adults. In other words, there is no database of adult exploitation materials that hashing software could rely on for screening purposes. One reason for this is likely that images of exploited adults are not illegal per se (i.e., images of non-exploited and exploited adults could ostensibly appear the same to a viewer, whereas images of children can be unequivocally designated as illegal); thus, it is more challenging to identify the images that would be included in a hash database without additional context or facts related to the image. Therefore, policymakers, instead of adopting policies and laws which would forbid the use of tech tools because of tools' shortcomings, should work with the private sector to adopt policies which would enhance the use of these innovative tools.

The ECC example highlights the need for regulation on mandatory monitoring and the precarious nature of current monitoring efforts. Under most existing approaches, law enforcement is entirely dependent on the voluntary, proactive detection efforts of the private sector. For example, the Draft Strategy discussed above includes the following observation: "[I]f one company—Facebook—stops voluntarily scanning its platform for CSAM, or if it lost the ability to do so because of its adoption of end-to-end encryption, the volume of CyberTips could instantly drop from over 20 million to less than 1 million. This sudden loss of investigative leads would create a whole new horror for law enforcement and the children they seek to rescue."

Moreover, although some large platforms have conducted detection efforts to generate substantial numbers of tips for law enforcement, many other platforms do not bring the same attention or resources to such efforts. Thus, voluntary frameworks foster an uneven playing field and potential safe havens for criminals. And finally, a voluntary or "goodwill" approach is risky for States because it is subject to the business's weighing of numerous competing interests, such as cost, resources, liability and competiveness.

– The growing use of encryption

The growing use of encryption technologies, in part driven by increasing privacy concerns, poses a significant investigation challenge to authorities in the context of technology-facilitated THB.

End-to-end encryption means that communications are securely protected, whereby content is only visible to the participants within a conversation. In the past, online platforms have been able to monitor content passing through their systems using tools, such as those described above, that automatically search for the presence of known child sexual abuse images. Encryption prevents such tools from accessing and analysing content, posing a significant obstacle to the ability of online platforms to monitor, filter, block or remove prohibited content that is being shared.

There are some automatic filtering tools that can be used in end-to-end encrypted services because they scan at the moment of sending rather than in transit. However, currently active scanning and filtering of child sexual abuse material and other illicit material linked to THB offences only occurs on services that are not end-to-end encrypted.[165] Human monitoring, pivotal to the identification of material linked to the commission of adult trafficking offences, which often require more nuanced analysis, is not possible for communications that are end-to-end encrypted.

Across the world, law enforcement authorities are faced with one of two options when seeking to access encrypted communications: attacking the encryption (by performing a lawful intercept or ap-

165 See Elizabeth Reeves and Simone Vibert, *Access denied: How end-to-end encryption threatens children's safety online* (Children's Commissioner for England, December 2020), p. 15.

See also 5Rights and Professor Hany Farid, *Briefing: end-to-end encryption and child sexual abuse material* (5Rights Foundation, December 2019), p. 5.

plying brute force) or bypassing it (by requiring the encryption key to be handed over). Legal provisions enable the latter approach in only four EU States – Belgium, Croatia, France and Ireland – and in the United Kingdom.[166] This highlights the fragmented approach being taken to govern the use of encryption; there is no homogeneous practice across the OSCE or sub-regions. Given the cross-border nature of a wide range of serious crimes, including many technology-facilitated THB offences, greater harmonization in legislative approaches taken to encryption is required to preserve the capacity to conduct cross-border investigations.

Encryption has already proven a significant obstacle in a wide range of criminal investigations. In Brazil, courts fined Facebook (as WhatsApp's parent company) for refusing to share data (protected by the application's end-to-end encryption) for use in a criminal investigation into drug trafficking.[167] The OSCE Mission to Montenegro highlighted the increasing encryption of digital devices as a key challenge for investigating technology-facilitated THB offences in that country.[168] Encryption was similarly highlighted by law enforcement in both the United Kingdom and Israel as a growing challenge being faced.

In October 2020, seven national governments – United States, United Kingdom, Australia, New Zealand, Canada, India and Japan – issued a joint statement expressing concern about the growing use of encryption technologies by tech firms, and requesting that companies move away from "end-to-end encryption policies which erode the public's safety online".[169] This follows previous concerns issued by the United States, United Kingdom and Australia in 2019 after Facebook's announcement that it would introduce end-to-end encryption for Facebook Messenger and Instagram.[170]

The EU's Strategy for a "more effective fight against child sexual abuse", published in July 2020, also highlighted encryption as a key and growing challenge in the context of online CSE. It further called for "solutions that could allow companies to detect and report CSAM in end-to-end encrypted electronic communications".[171] However, it is widely acknowledged that "back doors" built into encryption can be used by anyone and compromise the overall security of such communications. The adoption of automated screening technologies that can function in systems that are end-to-end encrypted can mitigate, although not entirely address, the challenges to monitoring posed by encryption.[172]

Taking a different approach, the Eurojust/Europol "Second Report of the Observatory Function On Encryption" identified homomorphic encryption as a way forward, as it "has the potential to solve the tension between having strong encryption while still allowing for lawful interception". The key benefit of homomorphic encryption is that it enables the analysis of encrypted data without decrypting it.[173] However, the significant computational capacity required to process this type of encryption poses an obstacle to its being widely adopted.[174]

Despite these consequences of encryption – and the lack of clear solutions - the technology industry, including social networking platforms, has been increasingly shifting towards use of end-to-end encryption due to a prevailing emphasis on privacy. Arguments have been put forward that encryption can also be beneficial to vulnerable groups by protecting their privacy. However, there is little disagreement that the impact of encryption on the monitoring of online platforms is likely to be vast. For example, in 2020, Facebook was responsible for 95% of the 21.4 million images and videos reported by technology companies to the US National Center for Exploited and Missing Children (NCMEC).[175] Were it to introduce end-to-end encryption across services, these reports would decrease drastically, removing a key source of data for NCMEC and law enforcement authorities in conducting investigations.

166 See Europol and Eurojust, *Second report of the observatory function on encryption* (Europol and Eurojust Public Information, 18 February 2020), p. 13.

167 See Gabriela Mello, "Brazil court slashes fine for Facebook's refusal to share WhatsApp data" [website] (Reuters, 25 June 2019). Available at: www.reuters.com/article/us-facebook-fine-brazil/ brazil-court-slashes-fine-for-facebooks-refusal-to-share- whatsapp-data-idUSKCN1TQ2RI (accessed 21 October 2021).

168 Written contribution by the competent authorities of Montenegro, 06 October 2020.

169 See US Department of Justice, "International Statement: End-To-End Encryption and Public Safety" [website] (US DOJ Office of Public Affairs, 11 October 2020). Available at: www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety (accessed 21 October 2021).

170 See Mark Zuckerberg, "A Privacy-Focused Vision for Social Networking" [website] (Facebook, 6 March 2019). Available at:

www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634 (accessed 21 October 2021).

171 See European Commission, *Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse* (Brussels: Publications Office of the European Union 24 July 2020), p. 2.

172 See Elizabeth Reeves and Simone Vibert, *Access denied: How end-to-end encryption threatens children's safety online* (Children's Commissioner for England, December 2020), p. 15.

See also 5Rights and Professor Hany Farid, *Briefing: end-to-end encryption and child sexual abuse material* (5Rights Foundation, December 2019), p. 3.

173 See Europol and Eurojust, *Second report of the observatory function on encryption* (Europol and Eurojust Public Information, 18 February 2020), p. 20.

174 Ibid.

175 See NCMEC, *2020 Reports by Electronic Service Providers (ESPs)* (NCMEC, 2021), p. 2. Available at: www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf (accessed 29 November 2021).

3. Content removal and blocking of websites

Closely related to the topic of monitoring is the issue of content removal – i.e., what a company does about prohibited content when it is notified of such content or discovers it during monitoring. This issue is central to the goal of mitigating harm to victims of exploitation.

Although a significant proportion of content-removal by online platforms is voluntary, many OSCE participating States have enacted regulatory frameworks requiring online platforms to remove certain content that has been detected and empowering State authorities to compel online platforms to block or remove content.

Some of the key variables in such regulations include the process for notifying companies of prohibited content; the process for defining whether the content is prohibited; the extent to which compliance is voluntary or mandatory; the timeline for take-down; whether the company notifies third parties such as law enforcements of the content; and enforcement mechanisms for compliance.

Central to this conversation is defining the content to be removed. Some approaches focus on requiring the removal only of illegal content, such as child sexual abuse material. However, there is increasing support for broader approaches that extend to content which is not per se illegal but that, for example, violates terms of use or otherwise causes harm. For purposes of this paper, such content is referred to as "prohibited" (as opposed to "illegal"). Examples of the latter might include fake job offers or escort ads which might not be actually illegal on their own but propose or invite an illegal act, or so-called "revenge porn" (aka non-consensual sharing of intimate images).

a. Reporting and notice

There are several components to notice and take-down processes, beginning with the report of prohibited content from a user. The reporting framework provided by platforms to users is important, since it can play a role in shaping the quantity and focus of reports.[176] For example, an analysis of the implementation of Germany's Network Enforcement Act (NetzDG) by online platforms found that if the NetzDG complaint tool was incorporated into the general complaints framework, there were far more reported take downs than when the complaints mechanism was positioned elsewhere or was less easily accessed.[177] This highlighted the importance of user accessibility in effective notification procedures.

A difference has been observed in the approach to notification procedures between larger technology platforms and smaller ones. Among larger players, including Facebook, Twitter, and Vkontakte, there is a degree of consensus regarding "general" notification procedures adopted for reporting. Among smaller operators, reporting procedures vary, meaning users may be less familiar with them and consequently submit fewer notifications.[178]

There is also significant variation in the categories of notifications users can submit to online platforms. For example, when reporting content to Facebook, users are asked to identify which of nine "problems" the content poses, or to choose "something else". Notably, though the "problems" include "nudity", "violence" and "false information", they do not explicitly refer either to CSE or THB. Only after choosing the "something else" option can users report "non-consensual intimate images" or "sexual exploitation". Although some THB dynamics arguably fall within existing categories (CSE and images depicting the services of victims of sex trafficking may fall within "nudity"; false job advertisements may fall within "false information"), they only do so implicitly, and rely on the awareness of the user to identify the appropriate category.[179] Additionally, although the processes for notification on Twitter and Vkontakte are similar, the notification categories provided are broader and quite different.[180]

The lack of express reference to THB or child sexual abuse in the reporting frameworks of key players may result in fewer user reports in relation to content linked to THB. NGOs and hotlines have argued that the notice and take-down provisions of some online platforms are not user-friendly enough, which artificially suppresses reporting.[181] Awareness-raising

176 NetzDG recognizes this by including an obligation on online platforms to provide an "easily recognisable, directly accessible and permanently available procedure for submitting complaints about unlawful content" (Section 3, 1, NtzDG). However, it did not provide further guidance on the structure of these procedures.

177 See Amélie Heldt, "Reading between the lines and the numbers: an analysis of the first NetzDG reports" *Internet Policy Review Volume 8 Issues 2* [website] (12 June 2019), p. 12. Available at: www.policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports (accessed 21 October 2021).

178 See Snapchat, "Information for Law enforcement" [website]. Available at: www.snap.com/en-US/safety/safety-enforcement (accessed 21 October 2021). In-app notifications for Snapchat require the user to hold down on the relevant material before the notification option appears.

179 See Facebook, "Report Something" [website]. Available at: www.facebook.com/help/263149623790594 (accessed 21 October 2021).

180 See Council of Europe, "Reporting on Social Media Platforms" [website] (Council of Europe). Available at: www.coe.int/en/web/no-hate-campaign/reporting-on-social-media-platforms#{"37117289":[4]} (accessed 21 October 2021).

181 See Alexandre De Streel et al, *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform* (European Parliament, June 2020), p. 10.

regarding appropriate notification procedures for users would be facilitated by greater consistency in reporting frameworks.

There are well-established examples of initiatives that facilitate the reporting of illegal content with the aim of achieving its removal. Two prominent initiatives are Insafe, a European network of Awareness Centres promoting safer and better usage of internet, and INHOPE. These two initiatives work together through a network of Safer Internet Centres (SICs) across Europe – typically comprising an awareness centre, a helpline, a hotline and a youth panel.[182] INHOPE, also supported by the EU Commission, is made up of 46 hotlines around the world that operate in all EU Member States, Russia, South Africa, North & South America, Asia, Australia and New Zealand to facilitate the removal of child sexual abuse material online that has been anonymously reported by the public. Serbia and Albania have hotline mechanisms outside the INHOPE network, while Bosnia and Herzegovina has a hotline inside the INHOPE network.[183] INHOPE also advocates for policy and legislative changes in the areas of THB for sexual exploitation of children online, and the generation of CSAM.

b. Determining illegality

Once platforms receive notice of content to be removed – either through third-party reports or monitoring – they will typically need to conduct an analysis of whether the content meets the criteria for removal. As discussed above, the content could be prohibited because it is illegal or because it violates a broader standard set by company policy or regulation. Even the issue of illegality can involve difficult questions for platforms, including what constitutes illegal content and who is responsible to confirm its illegality.

Where regulatory regimes require online platforms to take down content without a court order, this can create particular challenges in determining what content is illegal. This issue has been highlighted in the implementation of Germany's NetzDG,[184] which was principally enacted to address hate speech. As mentioned above, it requires social media platforms with over two million users to remove or block access to "manifestly unlawful" content within 24 hours of receiving a complaint.[185] If there is any doubt as to the legality of the content, seven days are permitted for a decision to be taken. The definition of "manifestly unlawful" refers to elements of the German Criminal Code. This includes CSAM, material depicting sexual abuse or coercion of adults, and any threat to commit THB offences.[186]

The inclusion of the term "manifestly", which implies judgment by the private sector company of whether content is lawful or not, lies at the heart of one strand of criticism of NetzDG: that it effectively transfers public responsibility to the private sector, which is left to determine whether content is "manifestly" unlawful.[187] This challenge is not uncommon. For example, Estonia's regulation requiring removal of illegal content is silent on who determines whether content is illegal.[188] Thus, where the provider/platform is given the preliminary responsibility of determining illegality, clear definitions of what constitutes "unlawful" content are required to limit uncertainty for the private sector.[189]

A second strand of criticism of regulatory frameworks, including NetzDG, requiring online platforms to take down reported content within short deadlines centres on concerns that such structures incentivize "over-blocking". This involves platforms agreeing to requests for taking down content which is not "manifestly unlawful", to avoid the possibility of sanctions. Such over-blocking risks limitations on free speech.[190] However, in the context of NetzDG, commentators have argued that take-down numbers in reports published by online platforms sug-

182 See Better Internet for Kids, "Insafe and INHOPE" [website]. Available at: www.betterinternetforkids.eu/policy/insafe-inhope (accessed 21 October 2021).

183 See Global Initiative Against Transnational Organized Crime, Preventing Vulnerability of and Strengthening Policy Responses For Commercial Sexual Exploitation Of Children In The Western Balkans (working title) – forthcoming.

184 See federal parliament of Germany, "Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)" (12 July 2017). The Network Enforcement Act, also known as NetzDG, focuses specifically on social networks (rather than platforms exercising editorial control over their content).

185 Emphasis on hate speech is set out in the Explanatory Memorandum (available at: www.dipbt.bundestag.de/doc/btd/18/123/1812356.pdf [accessed 29 November 2021]). Fines can be levied for a range of offences, including failure to provide and effectively monitor a system to appropriately handle user complaints. Sentencing guidelines suggest that the size of the network, the seriousness of the violation, whether the provider is a repeat offender, and co-operation of the provider all be taken into account when determining the size of the fine.

186 See Federal Parliament of Germany, German Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), sections 176, 177, 184b, 184d, s126.

187 See Amélie Heldt, "Reading between the lines and the numbers: an analysis of the first NetzDG reports" *Internet Policy Review Volume 8 Issues 2* [website] (12 June 2019), p. 4. Available at: www.policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports (accessed 21 October 2021).

188 See Parliament of Estonia, Information Society Services Act (RT I 2004, 29, 191, 14 April 2004), , § 11.

189 Clearer guidance could also shape the user terms and conditions imposed by private companies, which currently retain significant discretion in deciding what content is or is not admissible.

190 See Johanna Spiegel, "Germany's Network Enforcement Act and its impact on social networks" [website] (Taylor Wessing, August 2018). Available at: www.taylorwessing.com/download/article-germany-nfa-impact-social.html (accessed 21 October 2021).

For a commentary on the global concerns of over-blocking, see also Alexandre De Streel et al, *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform* (European Parliament, June 2020), p. 89.

gest that over-blocking has not occurred following the imposing of the NetzDG requirements.[191]

c. Removal

Once an online platform has been notified of the presence of prohibited content related to THB on their platform and, depending on the jurisdiction, that content has been confirmed as illegal or at least prohibited by an internal procedure of the company or another designated institution (law enforcement, or a specially designated NGO), the next step in the process is the removal of that content by the platform. There are no internationally recognized standards regarding the removal of content related to THB, including how quickly the content should be removed, who is responsible for taking the removal decisions, or whether the content should be shared with law enforcement authorities before removal.

Practices vary by country and across companies that host such material. In many jurisdictions, technology companies are not legally liable for third-party content uploaded on their platforms and thus the legal system does not oblige them to identify or remove such material. Under these circumstances, there is little incentive for online platforms to allocate financial and human resources in identifying and removing content related to THB.

In other countries, although there are no specific provisions regarding content related to THB or child sexual abuse and exploitation material, the removal of such content can fall under the general provision of online platforms being required to remove illegal content. Although this general rule should encompass the removal of any type of illegal material hosted on online platforms, this approach may also incentivize online platforms to prioritize other types of illegal content, such as violent extremism or terrorist activities, which often have a higher media profile. In situations where general frameworks are adopted, it is important that policymakers highlight the need to pay attention to content related to THB by issuing specific guidelines indicating how to identify and remove this type of content. One exception to the above legal approaches exists in the United States where US federal law requires US-based service providers to report instances of apparent "child pornography" that they become aware of on their systems to the National Center for Missing & Exploited Children's CyberTipline.[192]

There are several examples of State-led action on removal of content. For example, the European E-Commerce Directive makes its safe harbour regime (discussed above, p. 30) contingent on online platforms "expeditiously" removing or blocking content "upon obtaining such knowledge or awareness [of illegal content]".[193] The EU Commission Recommendations on tackling illegal content online provide further guidance by outlining proposals to be adopted by EU Member States and online platforms for the "expeditious" detection and removal of content, as well as prevention of its reappearance.[194]

In line with this, a number of States, including France, Hungary, Portugal and Germany, have enacted regulatory frameworks outlining processes that broadly stipulate the grounds upon which the removal or blocking of content may be mandated. These frameworks also name the competent judicial or administrative authority to issue such demands, and outline the related procedures. [195] This approach has also been adopted in non-EU OSCE participating States, including Turkey and the Russian Federation.[196]

However, the non-binding nature of the EU Recommendations on tackling illegal content online, and the lack of consensus around procedures for notifying and taking down content, mean a plethora of different approaches have been adopted by OSCE participating States. For example, the regulatory framework in Finland blends self-regulation with State-sanctioning powers, by envisaging that online platforms will voluntarily remove illegal content once they become aware of it, whether through their own due diligence or through reporting from individuals, without the need for judicial intervention. However, failure to do so can result in State-imposed penalties, although in practice these are limited by State awareness. In other jurisdictions, including Germany, once notified, online platforms are required to remove certain content within 24 hours, or face significant sanction.[197] However,

191 See Amélie Heldt, "Reading between the lines and the numbers: an analysis of the first NetzDG reports" *Internet Policy Review Volume 8 Issues 2* [website] (12 June 2019), p. 5. Available at: www.policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports (accessed 21 October 2021).

192 See NCMEC, "Is Your Explicit Content Out There?" [website]. Available at: www.missingkids.org/gethelpnow/isyourexplicitcontentoutthere (accessed 21 October 2021).

193 See European Parliament and Council, *Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)* (Official Journal of the European Communities L178/1, 17 July 2000), article 14 ECD.

194 The Recommendations also request online platforms to cooperate with authorities more closely, specifically by reporting evidence of serious criminal offences linked to illegal content.

195 See Council of Europe, *Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content* (Lausanne: Council of Europe, January 2017), p. 29.

196 Ibid.

197 Regarding Finland's approach, see OSCE, "Statement by Petya Nestorova, Executive Secretary of the Council of Europe Convention on Action against Trafficking in Human Beings", 19th Alliance against Trafficking in Persons: Panel 4 [website] (Vienna: OSCE, 18 April 2019). Available at: www.osce.org/cthb/420167 (accessed 21 October 2021), starting from 32:57.

many of these regulations lack clarity and the obligations they impose vary. This creates a fragmented compliance landscape for online platforms.

The powers of law enforcement related to content removal are also unclear in some countries. For example, in Montenegro, the Law on Electronic Communications does not clearly spell out the powers of law enforcement to compel the removal or blocking of internet content for websites, whether these are hosted within or beyond the country's jurisdiction. [198]

Even where regulations exist and are harmonized across jurisdictions, enforcing the take down of content is often a slow and, in the context of user-enforced take downs, an expensive procedure. Illustratively, the European Union's General Data Protection Regulation "right to be forgotten" applies across EU Member States, and was initially seen as a powerful tool for protecting individuals who have suffered from having sexually explicit images published online without their permission (also known as "non-consensual distribution of intimate images online"). Yet victims of such violations and legal professionals working to enforce their "right to be forgotten" report that these rights are extremely difficult to implement, with some online platforms being particularly slow or un-cooperative in responding to requests to take down content.[199]

The approach to establishing rules regarding the removal of THB content can be informed by experience related to other topics, such as terrorism or hate speech. For example, the EU Terrorist Content regulation requires that all online hosts must remove "terrorist content" within 60 minutes of notification. Germany's NetzDG obliges social networks to remove criminal content and illegal hate speech within a timeframe of 24 hours or face fines of up to €50 million. Also, as mentioned above, in accordance with the recently enacted Australian Online Safety Act 2021, depending on the contravening material, online service providers must comply with a take-down notice within 24 hours of receipt of that notice.

d. The challenge of jurisdiction in regulating content removal in the global online marketplace

National regulators across the OSCE face challenges of jurisdiction when seeking to compel the removal of content by platforms incorporated beyond their national borders. However, recent EU case law has clarified that orders issued by EU Member State courts have global reach. This is the case at least in law; methods of practical enforcement may pose more of a challenge.

An October 2019 ruling by the European Court of Justice (ECJ) specifically regarding Facebook concluded that online platforms can be compelled to remove content deemed defamatory or unlawful globally through orders issued by national courts of EU Member States. Prior to this judgement, domestic court orders were perceived by platforms to relate only to content available within the relevant country.[200] The 2019 ECJ judgment sought to address challenges relating to jurisdiction faced by national authorities, and demonstrates the increasing desire of the EU judiciary to improve online regulation.[201]

Nevertheless, in practice, as the transparency reports of Facebook and Youtube make clear, content is only taken down globally if it violates community guidelines. If it violates national laws, it is only "locally restrict[ed]".[202] It remains to be seen whether the EU Digital Services Act, particularly the requirements to appoint EU legal representatives (outlined at p. 30), will change this.

Spain has leveraged its data protection regime, which – in line with the EU GDPR – has significant extra-territorial reach to bypass, at least implicitly, these jurisdictional challenges. In 2019 the Spanish Data Protection Authority spearheaded an initiative in which it tasked the public – citizens of Spain or legal residents – with identifying and requesting the removal of sexually explicit or violent imagery, including CSE materials, on internet platforms.[203] If an individual's request is unsuccessful, or the harm of continued dissemination is deemed high, the public can contact the data-protection authority directly,

Regarding fragmentation within the EU, see Niombo Lomba and Tatjana Evas, *Digital services act: European added value assessment* (European Parliamentary Research Services, October 2020), p. 196.

198 Written contribution by the competent authorities of Montenegro, 06 October 2020

199 See Leonie Cater, "How Europe's privacy laws are failing victims of sexual abuse" [website] (Politico, 13 January 2021). Available at: www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/ (accessed 21 October 2021).

See also PermessoNegato, *State of Revenge* (November 2020). Available at: www.permessonegato.it/doc/PermessoNegato_StateofRevenge_202011.pdf (accessed 21 October 2021).

200 See InfoCuria Case-law, *Eva Glawischnig-Piesczek vs. Facebook Ireland Limited, October 2019, Case C-18/18* (Court of Justice of the EU, October 2019). Available at: www.curia.europa.eu/juris/document/document.jsf?docid=218621&doclang=EN (accessed 21 October 2021).

201 By contrast, in October 2019 the ECJ found that the EU's right to be forgotten, which compels internet service providers to remove all material regarding a particular individual, did not, in most cases, have a global reach. This demonstrates the careful tightrope judiciary must walk in making decisions regarding the extra-territorial reach of laws governing the internet.

202 See Google, "Removals under the Network Enforcement Law" [website]. Available at: https://transparencyreport.google.com/netzdg/youtube?hl=en (accessed 21 October 2021).

203 See Agencia Española de Proteccion de Datos, "Canal Prioritario" [website]. Available at: https://www.aepd.es/canalprioritario/ (accessed 21 October 2021).

which will review the request within 24 hours of receipt. If the authority finds the content to be harmful, it will demand that the platform promptly remove the content.

Failure to comply is sanctionable and platforms may face penalties for the dissemination of harmful material. The authority has already successfully demanded content removal by platforms outside of the European Economic Area, making it clear that the authority's mandate extends, at least in practice, globally. Platforms have been cooperative in this initiative, possibly driven by the threat of reputational harm stemming from public awareness of non-compliance.

In addition to amending policy and legislation to facilitate cross-border enforcement in the context of technology-facilitated THB, it is key that States leverage mutual recognition instruments that facilitate the recognition of legal decisions across borders, and reinforce implementing provisions. Mutual legal assistance treaties or agreements are good examples of such instruments. Their advantage is that they enable countries to collect and exchange information quickly, and to carry out specific legal procedures without additional bureaucracy. Since THB cases are time-consuming, the advantages of mutual legal assistance treaties or agreements are crucial to prompt investigation.

e. Taking down or blocking websites

A more substantive form of content removal is to take down or block the entire website where the prohibited content resides. This approach is most commonly done with regard to THB for sexual exploitation; initiatives seeking to block access to websites featuring false job advertisements, which can lure victims into situations of labour trafficking, have not been identified. There is a close and often intertwined relationship between THB for sexual exploitation and prostitution markets in general. The services of persons trafficked for sexual exploitation are typically procured within a broader prostitution marketplace, whether legal or illegal. With respect to technology-facilitated THB, traffickers regularly advertise their victims online next to other advertisements for sexual services. Since many websites do not conduct meaningful age or consent verification, traffickers are able to present their victims as willingly engaged in prostitution to sex buyers who are unwilling or unable to identify them as victims.

States have begun to address this challenge in a variety of ways. In certain countries, primarily where prostitution is entirely or predominantly illegal, States have sought broad powers to compel not only the removal of specific content, but the take down or blocking of entire websites identified as facilitating the provision of sexual services or the sharing of explicit content. While these approaches are clearly a more comprehensive response to prohibited content, they can operate as part of the toolbox for addressing technology-enabled THB.

Blocking sites has been a recognized practice particularly in the context of combating online child sexual exploitation. For example, the 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 requires Member States to "take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory," and grants States the option of taking measures to "block access to web pages containing or disseminating child pornography towards the Internet users within their territory."[204]

The application of this approach to adult services websites is more recent. In 2017, Israel passed the Powers to Prevent Online Offences Law, which empowers designated prosecutors to file requests to the district courts to deny access to, or shut down, websites dealing with trafficking in human beings, prostitution, pornography, online gambling, drug trafficking and terrorism.[205] The enactment was driven by a growing realization that the designated offences were increasingly shifting online, and that existing methods of blocking content were too slow since they were easily outpaced by websites re-appearing on different servers.[206] In line with this, the new Law provides an alternative route to shutting down websites, a route that sits outside criminal procedures and is far quicker: typically it takes from 2 to 3 weeks between a request for a restraining order being submitted and the website being taken down (when hosted within Israel) or access is restricted (for websites hosted outside the country, by blocking access or ensuring that they cannot be searched for). Labour trafficking falls outside the scope of this legislation, since labour trafficking is believed by authorities to involve a limited online element and to occur predominantly offline in Israel.[207]

204 See European Parliament and Council, "*Directive 2011/93/EU 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*" (13 December 2011), art. 25.

205 See Knesset of Israel, "*Law on Authorities for the Prevention of Committing Crimes through Use of an Internet Site, 5777-2017*" (Law on Authorities). Available at: www.fs.knesset.gov.il/20/law/20_lsr_390328.pdf (accessed 21 October 2021).

206 Telephone interview with Ayelet Dahan, Deputy Anti Trafficking Coordinator, Ministry of Justice of Israel, and Alexandra Karra, *Senior Attorney*, *Cybercrime Department*, State Attorney's *Office*, *Ministry* of Justice of Israel, 19 November 2020.

207 Ibid.

Israeli law enforcement has observed users of blocked websites shifting to less mainstream platforms, including encrypted services such as Telegram.[208] A connected shift in the modus operandi of relevant websites is publishing advertisements for prostitution on the surface web without any functionality to contact the individuals depicted, operating instead as "an online catalogue". A linked encrypted sister site, on Telegram in some cases, provides the contact functionality.[209] Between the enactment in 2017 of the Powers to Prevent Online Offences Law and November 2020, action has been taken against 36 websites publishing advertisements for prostitution. It is, however, unclear what proportion of these offered advertisements for the services of trafficked persons. In addition, nearly 3,500 websites depicting child pornography were blocked.[210]

Similarly, in Kazakhstan, a 2016 legislative reform simplified the process for suspending or blocking websites hosting pornographic or sexually explicit material for up to three months. Four designated agencies are able to block websites without requiring a court decision.[211]

The above examples highlight that laws and regulations can have different intents when addressing THB facilitated by websites. In countries like Israel, the primary focus is shutting down the website itself. In other countries or jurisdictions, as in the example of the Texas statute mentioned below at p. 48), the intent is to prosecute the operators of the websites. This is an important distinction, since it requires different approaches from law enforcement authorities and policymakers.

In the United Kingdom, a 2018 report on sexual exploitation in England and Wales by the All-Party Parliamentary Group on Prostitution and the Global Sex Trade found that adult services websites were "the most significant enabler of sex trafficking in the UK". Vivastreet and Adultwork were named as the two largest platforms.[212] This prompted widespread calls to ban adult services websites. This in turn triggered significant protests and pushback from groups representing persons in the sex industry.[213] Following extensive debates in the House of Commons, the United Kingdom opted against banning such websites. UK law enforcement authorities argued that outlawing such sites would remove a key source of intelligence used by authorities to track down THB networks and their victims.[214] They further claimed that any shift onto encrypted sites would pose an additional challenge.

Similarly, the Republic of Georgia's Unit on Combating Illegal Migration and Human Trafficking, part of Georgia's Central Criminal Police Department, uses online platforms advertising prostitution and pornography as key sources of intelligence when identifying THB cases. This includes conducting interviews with people in prostitution advertising their services to identify victims of trafficking.[215]

While recognizing the importance of law enforcement utilizing online information, advocates of shutting down websites used for advertising sexual services note that the intelligence gains of the police are far outstripped by the harms resulting from the expansion of marketplaces for the services of trafficked persons driven by adult services websites.[216] Further, they argue that the small number of successful investigations are outweighed by the harms experienced by far greater numbers of victims. And finally, they note that the websites have demonstrated little in the way of meaningful safety measures.

Research and practitioner experience has repeatedly confirmed that the internet underpins the business model of THB for sexual exploitation across a wide range of jurisdictions, including the United States, Europe, Central Asia and South East Asia.[217] Technology lowers barriers to entry for traffickers, who are easily able to advertise the services of trafficked victims while facing reduced risks, as well as buyers, who can simply and anonymously obtain a wealth

208 It is key to note that the aim of the law was primarily to tackle the publication of explicit material and its impacts on the Israeli society, rather than to target the publishers of the material per se. Consequently, although movement onto more encrypted platforms complicates investigation, it does limit exposure of the general public to such material, in line with the law's aims.

209 In one case where the prosecutors could show the linked sister site, the judge took down the surface website, regardless of the lack of contact functionality. Telephone interview with Ayelet Dahan, Deputy Anti Trafficking Coordinator, Ministry of Justice of Israel, and Alexandra Karra, Senior Attorney, Cybercrime Department, State Attorney's Office, Ministry of Justice of Israel, 19 November 2020.

210 Telephone interview with Ayelet Dahan, Deputy Anti Trafficking Coordinator, Ministry of Justice of Israel, and Alexandra Karra, Senior Attorney, Cybercrime Department, State Attorney's Office, Ministry of Justice of Israel, 19 November 2020.

211 See Ministry of Investments and Development of Kazakhstan, Resolution No. 60 of 25 January 2016 on the approval of the Regulations of co-operation of State authorities on compliance with the legislation of the Republic of Kazakhstan in the sphere of telecommunications, referring to The Law on Mass Media.

212 See All-Party Parliamentary Group on Prostitution and the Global Sex Trade*, Behind Closed Doors:*

Organised sexual exploitation in England and Wales (APPG, May 2018), p. 18.

213 See Lydia Morrish, "The rights of UK sex workers are under threat – why? Everything you need to know" [website] (Huckmag, 21 November 2018). Available at: www.huckmag.com/perspectives/reportage-2/the-rights-of-uk-sex-workers-are-under-threat-why/ (accessed 21 October 2021).

214 Telephone interview with Jessica Harrison and Victoria Tinker, UK Modern Slavery and Human Trafficking Unit, National Crime Agency, 19 November 2020.

215 Written submission by the Ministry of Justice of Georgia, 28 October 2020.

216 See Cross-Party Group on Commercial Sexual Exploitation, Scottish Parliament, *Online Pimping: Inquiry Findings Launched* [website] (CPGCSE, 19 March 2021), p. 22. Available at: www.cpg-cse.com/post/inquirylaunch (accessed 21 October 2021).

217 See OSCE and Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools* (OSCE, 22 June 2020), p. 14.

of information about a victim. Given that technology vastly amplifies the reach of traffickers, enabling them to target an expanded audience, and that technology companies do not have the necessary framework in place to ensure safety of users at scale, it is clear that current efforts to combat exploitation, especially on adult services websites and other high-risk platforms for THB purposes must be enhanced and policymakers should consider radical measures including taking down or blocking these websites.

Efforts to take down or block websites have to be comprehensive in order to have the desired impact. As we've seen in this section, in some countries authorities focus on shutting down websites. In other, the focus is on prosecuting the operators of websites. Future policy discussions should maybe consider both of these aspects, at the same time punishing operators and in parallel shutting down the platforms, evaluating which could be a more effective means of deterrence.

4. Liability for online platforms

As discussed above (Part D, 2 – Monitoring), two core, closely-connected principles have traditionally formed the basis for most existing regulatory approaches to online platforms: 1) no duty to monitor and 2) no liability for third-party content. The Council of Europe Recommendation contains a clear example of the latter: "States should ensure, in law and in practice, that intermediaries are not held liable for third-party content which they merely give access to or which they transmit or store."

a. Developing jurisprudence on liability

However, the principle on no liability is being challenged by recent jurisprudence and new legislation holding online platforms accountable – either from a civil or criminal perspective. One example is the United States' 2018 enactment of the FOSTA-SESTA package (which stands for Allow States and Victims to Fight Online Sex Trafficking Act [FOSTA] and Stop Enabling Sex Traffickers Act [SESTA] – hereinafter "FOSTA"). FOSTA sought "to clarify that section 230 of CDA [the Communications Decency Act] does not prohibit the enforcement against providers and users of interactive computer services of Federal and State criminal and civil law relating to sexual exploitation of children or sex trafficking."[218]

FOSTA notes that CDA section 230 was "never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[219] The clarification provided by FOSTA was required because CDA section 230 had been widely interpreted in practice and jurisprudence to provide such protection, leading to a lack of enforcement of criminal and civil laws against internet platforms.[220] The opening sections of FOSTA clearly lay out the intention of Congress and the flaws in the previous approach. This enables FOSTA to be leveraged not only as a legislative instrument, but as an advocacy tool.[221]

The impetus for the legislative change began in 2009, when the United States District Court for the Northern District of Illinois dismissed a case brought against the owners of Craigslist for hosting "erotic services", explicitly citing the protections offered by section 230 of the CDA.[222] This sparked a public awareness campaign and legal reform drive that culminated in the 2018 enactment of FOSTA.[223] The FOSTA legislative package clarifies that platforms are not immune from THB violations – from a federal criminal law perspective the position is unchanged – however it also enables civil claims against technology companies for financially benefiting from THB to move forward under The Trafficking Victims Protection Act.[224]

FOSTA drew significant backlash from advocates of internet freedoms, who saw it as an existential threat to the free working of the internet. The package also drew criticism from some groups representing persons in the sex industry, who argued that it pushed them back to the streets, exposing them to a greater risk of abuse.[225] At the same time, supporters of FOSTA, including victim-advocacy groups, argued that the websites did not provide greater safety to persons in the sex industry, but

218 FOSTA is specifically targeted at prostitution and sex trafficking, and excludes labour trafficking, organ trafficking, or other forms of exploitation related to trafficking.

219 See US Congress, *H.R.1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017* (Washington: U.S. Government Publishing Office, 4 November 2018), section 2.

220 Telephone interview with Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation, 8 December 2020.

221 See US Congress, *H.R.1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017* (Washington: U.S. Government Publishing Office, 4 November 2018), Section 2.

222 See Dart v. Craigslist, Inc., No. 09 C 1385 (N.D. Ill. Oct. 20, 2009). Available at: http://pub.bna.com/eclr/dartvcraigslist.pdf (accessed 21 October 2021).

223 See US Congress, *H.R.1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017* (Washington: U.S. Government Publishing Office, 4 November 2018).

224 Note that trafficking survivors have a civil claim not only against traffickers, but also those that financially benefit from their trafficking – this avenue is pursued by following liability from private sector entities, and can result in significant damages.

225 See Liz Tung, "FOSTA-SESTA was supposed to thwart sex trafficking. Instead, it's sparked a movement" [website] (WHYY, 10 July 2020). Available at: www.whyy.org/segments/fosta-sesta-was-supposed-to-thwart-sex-trafficking-instead-its-sparked-a-movement/ (accessed 21 October 2021).

rather profited off exploitation and benefited traffickers by providing platforms for exploitation, as evidenced by many confirmed cases of THB on websites.

Within 72 hours of enactment, a large number of websites offering escort and sexual services – including The Erotic Review, which had previously been identified as hosting content relating to the victims of sex trafficking – shut down their services for US users, while sites such as Craigslist made significant changes to their sections hosting classified ads related to the sex industry.

In July 2018, a few months following enactment, a US official stated that the package had enabled the government to "shut down nearly 90 percent of the online sex-trafficking business and ads."[226] While an investigation by the *Washington Post* found that an 82% drop in worldwide advertisements for sex in April 2018 had rebounded to 75% of their previous volume by July,[227] a sampling of online sex advertisements conducted in 2019 by ChildSafe.AI, a counter-THB technology company, found that almost 75% of these were duplicates, scams or spam.[228]

Contemporaneously with the enactment of FOSTA, the market-leading website Backpage.com – together with its owners – was indicated on numerous criminal charges, including THB.[229] It was immediately taken offline. The shutdown of Backpage triggered an immediate decrease in sex advertisements, an overall fragmentation of the adult services online industry, an increase in fake advertisements, and a shift towards using social media platforms – including Twitter and Instagram – for this purpose.[230]

Research conducted into the impact of FOSTA by Childsafe.AI one year after enactment found ongoing fragmentation of the online marketplace and sustained proliferation of fake advertisements, resulting in increased cost and decreased efficacy of online advertising for sex services, all of which raise barriers to entry.[231] FOSTA also drove a number of adult services websites to use Canadian or European servers, rather than US servers. This demonstrates the potential risks for patchy legislative reform to create safe havens, and highlights the potential benefits of multilateral approaches.

FOSTA has triggered at least 20 cases of civil litigation on behalf of THB survivors against private companies (both online and offline).[232] In a landmark judgement delivered in April 2020, a Texas Court refused to grant Facebook immunity under the Communications Decency Act from the claims of three victims of sex trafficking suing Facebook and Instagram for negligence, gross negligence and state law violations. The three women were groomed by traffickers on the platform as children. They alleged that Facebook does not do enough to mitigate the risk of sex trafficking on its platforms.[233] According to Facebook, this ruling is the first of 20 federal and state cases in Texas in which a court has not granted an online service provider's demand for immunity for content posted by third parties.[234]

The United States has also witnessed the first federal prosecution of a website for trafficking post-enactment of FOSTA. In June 2020, the website cityxguide.com ("CityXGuide") – a leading platform for online advertisements for prostitution and reportedly the venue of numerous instances of sex trafficking – was seized by Homeland Security Investigations pursuant to a warrant. The owner of the website had aspired to make CityXGuide the largest commercial sex advertising website after Backpage.com was taken offline in 2018, and was consistently unresponsive to law enforcement inquiries and subpoenas related to sex trafficking cases. Charges include promotion of prostitution and reckless disregard of sex trafficking, interstate racketeering conspiracy, interstate transportation in aid of racketeering, and money laundering.[235] In August 2021, Wilhan Martono, the owner of the website, pled guilty to Promotion and Facilitation of Prostitution and Reckless Disregard of Sex

226 See Statement by Rep. Ann Wagner (R-Mo.) in a video released by the House Judiciary Committee (20 July 2018). Available at: www.youtube.com/watch?v=Nfygwxz-IZs&feature=youtu.be (accessed 21 October 2021).

227 See Glen Kessler, "Has the sex-trafficking law eliminated 90 percent of sex-trafficking ads?" [website] (*The Washington Post,* 20 August 2018). Available at: www.washingtonpost.com/politics/2018/08/20/has-sex-trafficking-law-eliminated-percent-sex-trafficking-ads/ (accessed 21 October 2021).

228 See Rob Spectre, Childsafe.AI, *Beyond Backpage: Buying and Selling Sex in the United States One Year Later* (Childsafe.ai, 2019), p. 6.

229 See US Department of Justice, Office of Public Affairs, "Backpage's Co-founder and CEO, as well as Several Backpage-Related Corporate Entities, Enter Guilty Pleas" [website] (U.S. Department of Justice, 12 April 2018). Available at: www.justice.gov/opa/pr/backpage-s-co-founder-and-ceo-well-several-backpage-related-corporate-entities-enter-guilty (accessed 21 October 2020).

230 See Dan Whitcomb, "Exclusive: Report gives glimpse into murky world of U.S. prostitution in post-Backpage era" [website] (Reuters, 11 April 2019). Available at: www.reuters.com/article/us-usa-prostitution-internet-exclusive-idUSKCN1RN13E (accessed 29 November 2021).

Telephone interview with Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation, 8 December 2020.

231 See Rob Spectre, Childsafe.AI, *Beyond Backpage: Buying and Selling Sex in the United States One Year Later* (Childsafe.ai, 2019), p. 6.

232 Telephone interview with Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation, 8 December 2020.

233 See Cameron Langford, "Texas Court Refuses to Toss Sex-Trafficking Claims Against Facebook" [website] (Courthouse News Service, 28 April 20200. Available at: www.courthousenews.com/texas-court-refuses-to-toss-sex-trafficking-claims-against-facebook/ (accessed 21 October 2021).

234 Ibid.

235 See U.S. Attorney's Office, Northern District of Texas, "United States v. Wilhan Martono (CityXGuide) Case No. 3:20-CR-00274-N" [website] (USDOJ, 26 October 2021). Available at: www.justice.gov/usao-ndtx/united-states-v-wilhan-martono-cityxguide (accessed 29 November 2021).

Trafficking.[236] This case confirmed once again that criminals are regularly misusing online platforms to exploit people and casts doubt on arguments that websites are safe and do not contribute to THB.

In September 2019, in the United States, the State of Texas amended its Penal Code to include the offence of "online promotion of prostitution", making it an offence for "information content providers" to intentionally "promote the prostitution of another person or facilitate another person to engage in prostitution."[237] Together with FOSTA, which made it easier to target websites featuring sex advertisements, this indicates a similar intent to shut down online marketplaces for prostitution, although it does not establish pathways for shutting down the site outside criminal procedures.

More recently, in December 2020, following a *New York Times* article publicizing that Pornhub had hosted and profited from footage of child abuse and sex trafficking of adults, the "Survivors of Human Trafficking Fight Back" bill was introduced in the US Senate. The bill would criminalize hosting content depicting sex acts "knowingly or in reckless disregard of the fact that the participation of that person in the sex act was induced by fraud, force, threats of force, deception, or coercion", and empower sex trafficking victims, together with victims of revenge porn and sexual assault, to pursue civil claims against sites like Pornhub.[238]

Notably, this approach would move beyond criminalizing websites for – in essence – serving as accomplices of traffickers ("facilitating") to criminalizing the hosting of depictions that feature exploited persons, including adults. In other words, the bill aims to prevent the publication of content depicting persons who did not consent to the depiction. While the bill is at an early stage, it demonstrates gathering momentum in seeking to hold websites accountable for profiting from the exploitation of trafficked persons.[239]

Recent developments in Australian legislation have also changed the approach to the principle of monitoring and liability of online platforms. In 2021, Australian authorities enacted the Online Safety Act 2021 with the objective to improve and promote online safety for Australians.[240] The Act builds upon the existing online regulatory framework established in the Enhancing Online Safety Act 2015 and also introduces additional compliance obligations for companies operating online, including a set of basic, online safety expectations. Online platforms can now be required to give reports to the eSafety Commission in relation to their compliance with these expectations.

In accordance with the Act, electronic services providers can be asked by the eSafety Commission to remove - or take all reasonable steps to remove - content specified in the notice, take all reasonable steps to ensure contravening material is removed from the service, and – in certain circumstances - make access to that material subject to a further restricted access system. They can also be asked to link deletion notices to the provider of an internet search engine service to cease providing a link to certain material, and to issue app removal notices requiring the provider to cease enabling end-users to download an app that facilitates the posting of certain material on a social media service, relevant electronic service or designated internet service. Online service providers must comply with the takedown notice within 24 hours of receipt of that notice, decreased from the former 48-hour period.[241] Given the recent enactment of the Act, it is yet to be seen how it will be applied to THB situations. However, it appears that this new piece of legislation provides enhanced mechanisms for State institutions to address technology-facilitated THB, including with the active role of the technology industry.

236 Ibid.

237 See Senate Bill 20. Available at: www.capitol.texas.gov/tlodocs/86R/billtext/pdf/SB00020F.pdf#navpanes=0 (accessed 29 November 2021).

238 See United States Senate, Survivors of Human Trafficking Fight Back Act of 2020, section 2.

239 Although these challenges have predominantly originated from concerns surrounding sex trafficking, the erosion of immunity from liability could potentially create opportunities for greater enforcement against websites for other forms of exploitation, such as hosting false job recruitment advertisements, which are used to recruit victims into labour exploitation.

240 See Parliament of Australia, Online Safety Act 2021 No. 76, 2021. (Federal Register of Legislation, 17 March 2021).

241 See Hogan Lovells and Zachary Forrai, "A new era for Australian online safety regulation" [website] (JD Supra, 2 August 2021). Available at: www.jdsupra.com/legalnews/a-new-era-for-australian-online-safety-4740569/ (accessed 21 October 2021).

b. Challenges for establishing liability of online platforms

Criminal offences are generally composed of two elements: the act (*actus reus*), which can be established through act or omission, and the mental state (*mens rea*), namely, criminal intent, knowledge, recklessness or negligence. In the context of considering the liability of online platforms, it is the latter which raises particular challenges.[242] Liability typically rests either on the intentional commission of the offence by an individual or company, or on whether the organization or individual knew, or should have known (i.e., were apprised of facts that would lead a reasonable person to know), that the offence was committed using the company's services, products or infrastructure.

Given that few, if any, online platforms intentionally commit THB offences, the question usually depends on what the company knew or should have known about whether their platforms or services were being used for criminal purposes such as THB offences.

Illustratively, in the context of child sexual exploitation, the Lanzarote Convention requires State parties to criminalize conduct intentionally aiding or abetting the commission of the Convention offence of "distributing or transmitting child pornography".[243] The interpretation of when such facilitation is "committed intentionally" lies at the crux of the use of this provision to prosecute online platforms in practice.[244]

Determining the "should have known" standard for online platforms is the subject of debate in national courts. In the United States, the FOSTA-SESTA package clarified aspects of liability for online platforms that hinge on the "knowing" and "recklessness" standards. Its passage has triggered a range of cases analysing how to determine when private sector enterprises, including online providers, should become aware that their services are being used to facilitate THB (and they are therefore "knowingly" benefiting financially or "in reckless disregard of the fact"). [245]

It has been noted by advocates of a broad interpretation of the "should have known" standard that national courts play a key role in establishing liability in all contexts. Consequently, national courts are central in deciding whether an intermediary is liable, in providing protection against unfounded claims, and in enabling a body of case law to be built up to establish the way forward.[246] At the same time, for courts to take decisions in line with the intent of policy and lawmakers, laws and policies must be written clearly and comprehensively so there is little margin for inconsistency in jurisprudence.

An alternative way forward is to establish consensus on an objective "should have known" standard in order to facilitate enforcement of such provisions by reference to mandated due diligence thresholds. If such thresholds are not met, and an online platform is used for criminal purposes, this would create a presumption that the intermediary had the required awareness to be liable.[247] On the other hand, if the due diligence standards are met, typically the company would be immune from liability. The due diligence standards could be developed by a multi-stakeholder group, incorporating the technology sector as well as civil society and law enforcement, and could operate in parallel to enhanced transparency requirements to enable regulators to monitor compliance.

Linking liability to an objective due diligence standard was one element of the approach adopted in a recent draft of legislation in the United States called the EARN IT Act (Eliminating Abusive and Rampant Neglect of Interactive Technologies), which targets online child sexual exploitation.[248]

242 Since online platforms will almost never have "criminal intent" in committing an offence, the challenge lies in reaching consensus for "knowledge, recklessness, or negligence".

243 See Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote, 25 October 2007), article 1, 3 and 24. Note that the Convention enables national legislation to exclude the offence of accessing child pornography through ICT, together with the linked aiding/abetting offence, which would most explicitly appear to target intermediaries.

244 The debate specifically in relation to child sexual abuse material is further advanced than with trafficking in adults. For example, the Optional Protocol to the Convention on the Rights of the Child imposes obligations on States to establish the liability of legal persons for the sale of children, child prostitution and child pornography. This creates an opening for accountability of ISP and intermediaries, although the Protocol does not provide extensive detail as to how this should be achieved (Optional Protocol to the Convention on the Rights of the Child, on the sale of children, child prostitution and child pornography, adopted by Resolution A/RES/54/263 of 16 March 2001).

245 See Cameron Langford, "Texas Court Refuses to Toss Sex-Trafficking Claims Against Facebook" [website] (Courthouse News Service, 28 April 20200. Available at: www.courthousenews.com/texas-court-refuses-to-toss-sex-trafficking-claims-against-facebook/ (accessed 21 October 2021).

246 Telephone interview with Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation, 8 December 2020.

247 The obligations of the private sector to conduct due diligence to mitigate the risks of being involved in human rights abuses were most clearly set out in the UN Guiding Principles on Business and Human Rights and the "Protect, Respect and Remedy" Framework. Since 2010 there has been a trickle of legislation requiring businesses to conduct due diligence in their supply chains to mitigate the risk of human trafficking (usually in the context of trafficking for forced labour), this premised on the obligation to monitor and conduct due diligence. However, these supply chain monitoring requirements have not yet been linked to an objectively determined and mandated due diligence standard. Notably, a lack of clarity regarding the steps businesses should undertake has been identified as a weakness of many such laws. Mandating the parameters of a due diligence standard could offer the way forward in the context of both offline supply chains (while recognizing the complexity of applying one standard to a range of different sectors) and information service providers and online platforms. Recommendation CM/Rec(2018)2 of the EU Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies). Available at: www.search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680790e14 (accessed 29 November 2021).

The Act limits the CDA's section 230 blanket liability protection for online platforms with respect to claims of breaches of child sexual exploitation laws. It also establishes a National Commission on Online Child Sexual Exploitation Prevention, and directs this Commission to develop voluntary best practices for "interactive online services providers … to prevent online sexual exploitation of children."

The initial draft of the Act provided companies that complied with these "best practices" (including certifying such compliance to the Attorney General under a procedure established in the Act) a "safe harbour" from criminal or civil law suits relating to the misuse of platforms for commission of child sexual abuse offences.[249] This provision could have acted as a powerful incentive to companies in complying with these standards. However, although the Commission and best practices were retained in later drafts, the "safe harbour" was removed.[25]

c. Uneven approaches across countries

Regulatory change in the United States and European Union has significant ramifications globally, not only due to their influence in shaping regulation, but also because it is where many of the world's largest technology companies are based. However, the existence of regulatory approaches in a country hosting major technology companies should not serve as a reason for other countries not to adopt similar regulations. First, how technology is misused can differ from country to country, and regulatory solutions adopted by one country could be irrelevant to the problems of another. Second, a country cannot oblige a technology company to undertake certain actions within its jurisdiction in the absence of a regulatory framework, even if such actions are mandatory for the company based on the laws of another country. Therefore, coordinated regional and international action is required to ensure that technology companies are subject to laws and regulations in as many jurisdictions as possible. Additionally, such regulatory action has to be harmonized across jurisdictions to avoid creating conflicts or patchworks of laws.

5. Transparency regarding online platform actions

Public accountability of online platforms in addressing technology-facilitated THB is a very important element because in the absence of strong policies and laws in this field, one of the few mechanisms to incentivize technology companies to improve their response to online exploitation is through public pressure from civil society, media, THB survivors and others. In this regards, accountability is not possible without a high degree of transparency from online platforms on how they are addressing technology-facilitated THB at different levels. Transparency specifically refers here to disclosing actions related to policies adopted, algorithms implemented, processes designed, number of complaints received and how these complaints are being handle, number of THB cases identified and how they are being handled.

The vast majority of substantive online platforms have transparency policies, and many large online platforms publish annual or biannual transparency reports.[251] Although there has been an overall trend toward including more information in such reporting, reporting approaches vary, which complicates comparing platforms, and they are often insufficiently granular, which limits their value.

This situation was recognized by a significant proportion of respondents to a 2016 consultation conducted by the European Commission on the effectiveness of the European E-Commerce Directive, which called for greater transparency of content restriction policies among online platforms.[252] These responses have been reflected in the proposed EU Digital Services Act – as outlined above, p. 30.[253] However, in the absence of commonly accepted reporting requirements, EU Member States have started to legislate unilaterally, further fragmenting the legal regime.

A key example of this is Germany's above-mentioned NetzDG law, which imposes enhanced transparency obligations on companies. The Ex-

248 See US Congress, S.3398 – Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 or the EARN IT Act of 2020, introduced in the Senate of the United States on 5 March 2020.

249 See Committee on the Judiciary, "Chairman Graham Applauds Senate Judiciary Committee for Unanimously Approving the EARN IT Act" [website] (US Senate, 2 July 2020). Available at: www.judiciary.senate.gov/press/rep/releases/chairman-graham-applauds-senate-judiciary-committee-for-unanimously-approving-the-earn-it-act (accessed 21 October 2021).

250 See Amendments to the S.3398 – 116th Congress (2019–2020), Calendar No.491, 116th Congress, 2D Session. Available at: www.congress.gov/bill/116th-congress/senate-bill/3398/text (accessed 29 November 2021).

See also Riana Pfefferkorn, "House Introduces Earn It Act Companion Bill, Somehow Manages to Make it Even Worse" [website] (Stanford Law School, the Center for Internet and Society, 5 October 2020). Available at: www.cyberlaw.stanford.edu/blog/2020/10/house-introduces-earn-it-act-companion-bill-somehow-manages-make-it-even-worse (accessed 21 October 2021).

251 See Alexandre De Streel et al, *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform* (European Parliament, June 2020), p. 44.

252 See Martin Husovec and Ronald Leenes, Tilburg Institute for Law, Technology and Society, *Study on Role of online intermediaries: Summary of the public consultation* (Luxembourg, Publications Office of the European Union, 2014), p. 56.

253 See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC* (Brussels: Publications Office of the European Union, 15 December 2020), art (39).

planatory Memorandum states that this increased access to data will lay the groundwork for improving regulation in the long term.[254] NetzDG requires social networks receiving over a hundred complaints per year regarding unlawful content to publish biannual reports detailing how these complaints are handled. It also dictates a range of transparency requirements, including the time taken to respond and the nature of the complaints.

However, in reports published to date by online platforms pursuant to NetzDG, it is unclear which "take downs" relate to THB offences. While "take downs" for child sexual exploitation are detailed separately in several reports, those for adult THB could fall within a range of categories, including "sexually explicit" content, or material inciting the "commission of a felony".[255] It therefore remains difficult to assess the actions taken by online platforms to mitigate the risks of misuse for committing THB offences. Pending amendments to NetzDG include provisions seeking to enhance the value of information provided in platforms' transparency reports, including regarding platforms' automated procedures for detecting and deleting illicit content.[256]

The UK Online Harms position papers also incorporate a range of commitments aimed at greater transparency in reporting by online platforms, specifically regarding the procedures implemented to block and remove illicit and harmful content.[257] The White Paper, one of the position papers published by the UK Government, includes an indicative list of information categories to be included in transparency reporting, such as details of proactive use of technology tools to remove illicit and harmful content, and evidence of reactions to notification. Ofcom, the regulator of the new regulatory framework, will be required to publish further guidance on the elements of information that online platforms should include in their transparency reports.[258] The UK Government has also established a multi-stakeholder Transparency Working Group, which includes representatives from civil society and the technology sector, to further explore how online platform transparency can be enhanced. One Working Group recommendation for platforms, ahead of the Online Harms legislation coming into force, is to improve their reporting regarding Child Sexual Exploitation and Abuse data.[259]

A more harmonized framework governing online platforms' transparency obligations, both across the OSCE region and globally, would enhance the understanding of both law enforcement and the public regarding the role played by such intermediaries in illicit markets, including THB, and enable design of more effective regulatory frameworks. Such frameworks should be developed in consultation with online platforms, to balance the value of granular detail on the take down of content relating to THB and other offences against the reporting burden on platforms.

6. Findings on policy approaches to online platforms

The widespread misuse of technology by human traffickers continues to grow, manifesting on a diverse array of services and platforms as grooming and recruitment, power and control over victims, and exploitation through depictions, live-streaming or advertisements.

This growing challenge has been facilitated by inadequate protections across the technology sector. While some companies have developed measures or tools to respond, the reliance by countries on self-regulation coupled with voluntary compliance has resulted in fragmented and inadequate adoption of safety measures, inconsistent and slow reporting to authorities, lack of redress for victims, and impunity for traffickers. In short, the current policy approach by States to allow self-regulation by the technology sector has not worked to stem the tide of online exploitation.

Recognition of these shortcomings is fuelling a call for State-led regulation based on mandatory compliance. Technology-facilitated THB requires strong legislative action by governments to establish industry standards, harmonize approaches, support enforcement and protect victims. Policy development should involve input from the technology sector and civil society and take into account the unique characteristics of different platforms, but State-led intervention is critical.

The analysis above highlights that, as part of the shift toward comprehensive State-led regulation,

254 See Federal Parliament of Germany, Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) (12 July 2017), section 2.

255 See Facebook, *NetzDG Transparency Report 2020* [website] (Facebook, July 2020), p. 5. Available at: www.about.fb.com/wp-content/uploads/2020/07/facebook_netzdg_July_2020_English.pdf (accessed 21 October 2021).

256 See Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes. Available at: www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Aenderung_NetzDG.pdf;jsessionid=D8952A9C53BA2715E7C504D2C0BE7A44.2_cid297?__blob=publicationFile&v=2 (accessed 21 October 2021).

257 See UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper: Full Government Response to the consultation* (UK Government, December 2020), p. 67.

258 See UK Government, Department for Digital, Culture, Media & Sport and Home Office, *The Government Report on Transparency Reporting in relation to Online Harms* [website] (UK Government, 15 December 2020), p. 3.2. Available at: www.assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944320/The_Government_Report_on_Transparency_Reporting_in_relation_to_Online_Harms.pdf (accessed 21 October 2021).

259 Ibid

policy makers will need to address several core issues relevant to THB. First, several States are exploring "safety by design" policies to work upstream preventing harm. Such measures are promising but still in the early stages of adoption. For example, age verification has seen increased attention in recent years, but the focus has been mostly confined to verifying the ages of visitors to websites, not the ages of persons depicted in sexually explicit content.

Second, as with the system of self-regulation generally, there is a growing recognition that the principle of "no duty to monitor" should be re-evaluated. A combination of robust human and technology-assisted monitoring is necessary to reduce the uploading and dissemination of harmful content by motivated actors. As part of this shift, approaches to other policy topics like privacy and encryption will need to be assessed in parallel.

Third, States will also need to establish clear parameters for removal of prohibited content, including requirements for companies to establish easily accessible mechanisms for the public to request content removal by the company, as well as for the companies to report to authorities while retaining the content for investigations. Clear standards on what content is to be removed are also needed, with government holding a central responsibility to define that content for companies. Countries are also increasingly taking more stringent action including blocking or taking down websites entirely.

Fourth, another historical tenet – no liability for third party content - is likewise being challenged in recent legislation and jurisprudence. This reflects a growing acknowledgment of the scale and severity of the problem, as well as the belief that victims need avenues to seek compensation for harm and authorities require tools to enforce due diligence obligations.

Finally, transparency has been increasingly recognized as fundamental for developing good policy and ensuring robust and good faith efforts by companies.

As noted above, a number of countries have begun to take initial steps toward State-led regulation. Current efforts, such as those underway in the UK and EU, are addressing some of these core issues such as reporting, monitoring and transparency, but still have limitations. For example, current State-led efforts are focused only on specific conduct and do not account for THB. Others focus only on illegal content and do not address other content which might be harmful. Most efforts to date have prioritized reactive identification and removal of previously-known child exploitation material; actions to proactively prevent the dissemination of new material, to prevent grooming and exploitation, and to implement default safety measures have been much less common. Most worrisome, is that initiatives to address online exploitation of adults are almost completely absent, even though adults represent two-thirds of all identified victims.

Thus, there is ample room for more effective and ambitious State-led regulation that will prevent harm and enhance safety online. Additionally, thoughtful, inclusive and harmonized policy development can create a more predictable, consistent and fair environment for businesses while ensuring there are no safe havens for exploiters.

260 See Madhumita Murgia and Martin Coulter, "Big Tech attacks UK plan to hold firms liable for harmful content" [website] (*Financial Times*, 1 July 2019). Available at: www.ft.com/content/3de70dd4-99ba-11e9-8cfb-30c211dcd229 (accessed 21 October 2021).

PART E Conclusions and recommendations

As technology becomes ever more central to both licit and illicit marketplaces, the challenge posed by technology-facilitated THB is only set to increase. Traditional methods of regulating technology have proved inadequate to the task and updated, effective policy responses are urgently needed. Solutions cannot be fragmented, un-coordinated and disproportional to the problem they are intended to counter; they must be comprehensive, scaled, sustainable and cost-efficient. An impactful response to technology-facilitated THB must be based on strong policies and legislation adopted by governments, with input of technology companies. In this regard, the Office of the OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings recommends that OSCE participating States consider the following aspects in developing policies in relation to technology-facilitated THB.

Ensure that technology-facilitated THB is covered by national definitions of THB and criminal procedure applicable to THB

Governments should ensure that criminal laws cover technology-facilitated THB, and that investigators and prosecutors have the necessary procedural tools to do their jobs, including investigation, collection of evidence, sharing information and presenting evidence in court. OSCE participating States should:

1. **Review national laws that are pivotal to enforcing and prosecuting technology-facilitated THB offences to ensure that they adequately apply to technology-facilitated THB offences and are in line with international standards as set out, at minimum, in the Budapest Convention. Relevant laws include: criminal codes, criminal procedure codes, rules of evidence, cybercrime legislation, and legislation regulating online platforms (including their data-sharing obligations), also bearing in mind the sector-specific challenges and possible sector-specific solutions. Criminal procedure codes in particular must allow for online investigations as well as the seizure and use of e-evidence in cases.**

2. **Consider whether inclusion of an explicit reference to technology-facilitated THB in anti-trafficking legislation is needed (for example, have prior cases of technology-facilitated THB been dismissed by courts on the basis that the statute did not cover technology-facilitated crimes?), or, alternatively, consider providing interpretative guidance confirming that existing legislation covers technology-facilitated THB. Such steps will provide greater certainty and clarity.**

   - Although few of the practitioners or stakeholders interviewed provided specific examples of existing legislation that does not cover technology-facilitated THB, explicit references to it or guidance could help avoid outcomes being left to interpretation and criminals avoiding accountability.

   - Highlighting the misuse of technology in anti-trafficking legislation could also provide significant value in terms of awareness-raising and norm-setting. In turn, this could lead to more attention being given to the topic, including in terms of resources. Although drafting must be done carefully to avoid unintended consequences, explicit references to technology should be considered as a feature of international, regional and national anti-trafficking legislation.

   - When drafting legislation or interpretative guidance regarding technology-facilitated THB—especially when it requires or recommends certain actions for technology companies--OSCE participating States should take into account sector-specific challenges and risks. For example, standards and measures vis-à-vis adult services or escort websites, where the risks of THB are high, may be different than in the case of search engines or online payment systems.

3. **Increase adoption of the Budapest Convention by all States and amend the Budapest Convention to expand its application to human trafficking cases.**

   - There is a need for a high degree of enforcement inter-operability across nations in addressing internet-based crimes. In the absence of an international instrument governing cybercrime (and in recognition that the status quo appears unlikely to shift in the short-term),[261] widespread adoption of the Budapest Convention is encouraged to advance a harmonized approach to responding to technology-facilitated child sexual exploitation. Currently the Budapest Convention has only 64 signatories; non-signatories remain beyond the scope of key obligations governing regulation and co-operation in addressing cybercrimes. Widening the Convention to apply explicitly to a broader

range of illicit activities, including THB, would also enhance awareness and may facilitate enforcement. Currently, nine OSCE participating States are not signatories to the Budapest Convention.

Enhance State-led regulatory frameworks

The overarching questions facing policy makers in the area of technology-facilitated THB are whether to choose self-regulation, co-regulation or State-led regulation, and whether to adopt voluntary or mandatory compliance regimes.

In the area of technology-facilitated THB, negative features of self-regulation have included: limited or non-existent industry standards; inconsistent and inadequate adoption and application of voluntary principles; and slow responses to documented abuse, failure to report abuse, or active complicity in facilitating exploitation from certain segments of the industry, particularly higher risk sectors like pornography, sexual services, short-term job seeking and social media. Abuse and exploitation have accelerated dramatically, but the industry's response as a whole has not kept pace, as indicated by the growing volume of technology-facilitated exploitation. States need policy tools to compel online platforms to mitigate the risk of their services being misused to commit THB offences, and to hold such platforms accountable for non-compliance. To ensure a level playing field and avoid safe havens for perpetrators, such policy tools must be based on mandatory compliance and be applied industry-wide, taking also into account the sector specific challenges and risks.

Thus, although good examples of innovation, partnerships and even policy have been developed under self-regulation approaches, it is the unequivocal conclusion of this report that co-regulatory or State-led regulatory frameworks featuring at least some mandatory compliance regimes are desperately needed. Nonetheless, a phase-in process that begins by codifying appropriate due diligence in non-binding regulation could be a useful, interim step. This could help in establishing consensus, as well as in creating space for exchanging knowledge and good practices, as well as incorporating lessons learnt.

Policy action from States should feature:

4. **Regional or harmonized approaches. Divergent national approaches can lead to piecemeal responses that are difficult for the private sector to comply with. They also risk creating safe havens for perpetrators. Existing laws, such as the U.S. FOSTA-SESTA, the Australia Online Safety Act or the proposed EU Digital Services Act, although very different in their approaches, have the potential to serve as a good basis for setting broader standards. They can also ensure that regulatory frameworks are suitable for governing online platforms in the context of THB and exploitation.**

5. **Regulatory reform that is based on co-regulation or State-led regulation. This should include robust mandatory obligations on core responsibilities, opportunities for industry input and self-regulation where appropriate and feasible, and liability for harm caused. Specifically, online platforms should be required to:**

   a. Establish safety as a paramount consideration for all categories of users (e.g. children and adults) in policy and regulatory measures (whether self-, co-, or state-led regulation). This should be done in tandem with other fundamental freedoms and rights such as privacy, however, safety should not be deprioritized relative to privacy in policy. Further, attention must be given not only to exploitation of children, but also of adults since the majority of human trafficking victims exploited through the misuse of technology are adults and mechanisms for their protection online are currently lacking.

   b. Implement "safety-by-design" principles in design, development and distribution phases. Principles should be developed in consultation with the technology industry. For example, default settings for privacy features should be set to prevent access to children on social media platforms.

   c. Adopt prevention measures which should include:

   i. Clear Terms of Use that could better serve as a deterrent, including simple language with key principles highlighted and that allow for removal of content and termination of accounts.

   ii. Age-verification for, at minimum: 1) visitors of websites with age-inappropriate content; 2) those uploading content to higher-risk sites such as sexual service sites or pornographic sites; and 3) critically - those depicted in sexually explicit materials. The uploader and the person depicted in the content may not be the same person, especially in cases of trafficking or exploitation of children. These standards should be applied to any platform that intentionally allows such content, not only platforms dedicated to such content (for example, some social media platforms have allowed such content without any verification metrics[262]).

261 See Summer Walker, *Cyber-insecurities? A guide to the UN cybercrime debate* (Geneva, Global Initiative against Transnational Organized Crime, 4 March 2019), p. 5.

262 See United States District Court, Northern District of California, Case No. 3:21-cv-00485-JCS John Doe #1 and John Doe #2 vs. Twitter, Inc. (04 July 2021). Available at: www.endsexualexploitation.org/wp-content/uploads/Doe-v-Twitter_1stAmndComplaint_Filed_040721.pdf (accessed 21 October 2021).

iii. In line with 5.c.ii, consent verification mechanisms should be explored for pornographic/sexually explicit content that is uploaded to any platform prior to its distribution.

iv. A clear, high visibility content-removal request mechanism for non-consensual, sexually explicit materials. The mechanism should be victim-centred where the onus is placed on the uploader to affirmatively prove consent to have the material re-instated.

d. Conduct regular due diligence of their operations and systems based on concrete standards to identify risks of misuse of their platforms and resources by traffickers and to mitigate risks that are found. Governments need to take responsibility to guide the development of such due diligence standards, preferably through multi-stakeholder consultations that include the technology industry, civil society, victims and law enforcement. Due diligence standards should include risk assessment at all phases from design to distribution and use of products, include attention to risk mitigation strategies, and take into account the sector specific challenges and risks.

e. Conduct proactive monitoring for exploitative materials and misuse of platforms, and establish mechanisms that allow direct reporting by the public to companies. Governments should support companies with clear guidance on the obligations of companies with regard to monitoring, including the materials or activities to be identified. Companies should be encouraged to examine material based on risk, rather than illegality alone. Here, the focus on harm rather than illegality in the UK Online Harms Bill provides food for thought. The Bill defines "harmful" as content that the "service provider would have reasonable grounds to believe" poses a "material risk" that it may have "a significant adverse physical or psychological impact on an adult of ordinary sensibilities." Such approaches allow for better recognition of harder-to-identify exploitation of adults. However, it should be noted that policy makers must strive for as much clarity and definition as possible to reduce the requirement for difficult judgments by companies. Features of the monitoring framework should include:

i. Requirements to remove content expeditiously, by using both artificial intelligence tools and human moderation, and to preserve it securely for possible use in investigations or prosecutions.

ii. Provisions to report content to appropriate/designated authorities. Governments must provide for a designated agency or authority to receive and act upon such reports.

iii. An enforcement mechanism for failure to comply. Such mechanisms should be focused on achieving/incentivizing the above goals rather than on punitive sanctions.

f. Establish liability for harm caused by content on the platforms or exploitation on the platforms based on the should-have-known principle. Under this principle those harmed by content or exploitation on online platforms would be able to file a civil lawsuit against the platforms and seek damages. This principle is also a good incentive to determine companies to "go the extra mile" in addressing technology-facilitated THB;

g. Establish transparency standards regarding the reporting of platform misuse, the procedures used by online platforms to mitigate the risk of their services being misused, and the outcomes of such efforts. Greater data collection and synthesis is needed to support policy development.

6. **Self-regulatory aspects and co-operative approaches can be promoted in parallel to corresponding State-led policy actions. Examples of self-regulatory, co-operative or sector-initiated actions could include:**

a. Promoting industry-led enhanced safety and safeguarding measures, including by establishing industry-led associations or other multi-stakeholders approaches to share good practices and promote innovation.

b. Continuing to promote, facilitate and strengthen child safety referral services and helplines.

c. Investing in evolving voluntary, automated filtering and blocking tools to mitigate the risk of misuse of services.

d. As noted in 5.e. above, developing industry approaches to material that is not necessarily illegal, but still potentially harmful.

e. Invest resources to ensure an adequate level of human moderators recognizing that this aspect will differ depending on the risk profile of a service and other factors.

7. **Enhanced co-operation between States, the private sector and civil society.**

a. Develop national guidelines on institutionalized monitoring and coordinated data gathering and sharing between law enforcement, anti-trafficking actors/child protection system actors, and other relevant stakeholders. Such guidelines could focus on multidisciplinary use of tools, such as the Interpol-hosted ICSE database. States should also invest in mapping the online landscape, assessing risks of technology-facilitated THB, and gathering data on the nature and scale of the challenge, to build the evidence base for better policy development.

Annex 1 – Selected List of Policies and Regulations

Legislation

International and Regional Instruments

Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (Palermo Protocol)	Adopted by Resolution A/RES/55/25 of 15 November 2000 and entry into force in 25 December 2003, in accordance with article 17	www.ohchr.org/Documents/ProfessionalInterest/ProtocolonTrafficking.pdf
Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography	Adopted by Resolution A/RES/54/263 of 16 March 2001 and entry into force in 18 January 2002, in accordance with article 14(1)	www.treaties.un.org/doc/Treaties/2000/05/20000525%2003-16%20AM/Ch_IV_11_cp.pdf
Convention on the Elimination of All Forms of Discrimination against Women	Adopted and opened for signature, ratification and accession by General Assembly resolution 34/180 of 18 December 1979 entry into force 3 September 1981, in accordance with article 27(1)	www.ohchr.org/Documents/ProfessionalInterest/cedaw.pdf
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)	Opening of the treaty on 25 October 2007 and entry into force on 1 July 2010 (5 Ratifications including at least 3 Member States of the Council of Europe)	www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201
Convention on Cybercrime (Budapest Convention)	Opening of the treaty on 23 November 2001 and entry into force on 1 July 2004 (5 Ratifications including at least 3 Member States of the Council of Europe)	www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market	8 June 2000	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

Selected National Laws

Albania	Criminal Procedure Code of the Republic of Albania	21 March 1995	www.legislationline.org/download/id/8236/file/Albania_CPC_1995_am2017_en.pdf
Australia	Cybercrime Act 2001	21 Dec 2001	www.legislation.gov.au/Details/C2004A00937
Australia	Online Safety Bill	4 February 2021	www.legislation.gov.au/Details/C2021B00018/Explanatory%20Memorandum/Text
Estonia	Information Society Services Act	14 April 2004	www.riigiteataja.ee/en/eli/515012019001/consolide
Germany	Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)	12 July 2017	www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=82%209D39DBDAC5DE294A686E374126D04E.1_cid289?__blob=publicationFile&v=2%20Ibid
Germany	German Criminal Code	13 Nov 1998	www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html
Israel	Penal Law (Law 5737-1977)	7 June 1977	https://knesset.gov.il/review/data/eng/law/kns8_penallaw_eng.pdf
Israel	Law on Authorities for the Prevention of Committing Crimes Through Use of an Internet Site	17 July 2017	www.fs.knesset.gov.il/20/law/20_lsr_390328.pdf
Moldova	Criminal Code of the Republic of Moldova	18 April 2002	www.legislationline.org/download/id/3559/file/Criminal%20Code%20RM.pdf
Moldova	Law 20/2009 on preventing and combating cybercrime	26 January 2010	www.legis.md/cautare/getResults?doc_id=106547&lang=ro
Montenegro	Electronic Communications Act	13 August 2013	www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=148089&rType=2&file=Law%20on%20Electronic%20Communications%20ispravka.pdf
New Zealand	Harmful Digital Communications Bill 2013	27 May 2014	www.parliament.nz/en/pb/bills-and-laws/bills-digests/document/50PLLaw21661/harmful-digital-communications-bill-2013-2014-no-168-2
Spain	Criminal Procedure Code	3 January 1983	www.boe.es/buscar/act.php?id=BOE-A-1882-6036&p=20200930&tn=1
United Kingdom	Modern Slavery Act 2015	26 March 2015	www.legislation.gov.uk/ukpga/2015/30/contents/enacted

Ukraine	Law on Telecommunications	18 Nov 2003	www.wto.org/english/thewto_e/acc_e/ukr_e/WTACCUKR98A13_LEG_1.pdf
United States	S.3398 – EARN IT Act of 2020	5 March 2020	www.congress.gov/bill/116th-congress/senate-bill/3398/text
United States	H.R.1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017	11 April 2018	www.congress.gov/bill/115th-congress/house-bill/1865/text
United States	S.1693 – Stop Enabling Sex Traffickers Act of 2017	1 October 2018	www.congress.gov/bill/115th-congress/senate-bill/1693
United States	S.1312 – Trafficking Victims Protection Act of 2017	21 Dec 2018	www.congress.gov/bill/115th-congress/senate-bill/1312/text
United States	18 U.S. Code § 2251 – Sexual exploitation of children	3 January 2012	https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap110-sec2251
United States	18 U.S. Code 2258A - Reporting requirements of electronic communication service providers and remote computing service providers	3 January 2012	https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap110-sec2258A
United States	H.R.1761 – Protecting Against Child Exploitation Act of 2017	5 June 2017	www.congress.gov/bill/115th-congress/house-bill/1761/text?q=%7B%22search%22%3A%5B%22Steve+Scalise%22%5D%7D
United States	US Communications Decency Act 1996	8 February 1996	www.uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)
United States (State of California)	California Transparency in Supply Chains Act of 2010 Senate Bill No. 657 An act to add Section 1714.43 to the Civil Code, and to add Section 19547.5 to the Revenue and Taxation Code, relating to human trafficking	30 Sept 2010	www.leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200920100SB657
United States (State of Texas)	Senate Bill 20	22 May 2019	www.capitol.texas.gov/tlodocs/86R/billtext/pdf/SB00020F.pdf#navpanes=0

Policy

Multilateral

Council of Europe	Internet governance strategy 2016–2019	30 March 2016	www.rm.coe.int/internet-governance-strategy-2016-2019-updated-version-06-mar-2018/1680790ebe
Council of Europe	Recommendation CM/Rec (2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries	7 March 2018	www.search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14
European Commission	EU strategy for a more effective fight against child sexual abuse	24 July 2020	www.ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf
European Commission	Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC	15 December 2000	www.ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital
OSCE	OSCE Action Plan to Combat Trafficking in Human Beings, as amended	24 July 2003, 6 December 2013	www.osce.org/odihr/23866 www.osce.org/files/f/documents/f/6/109532.pdf
OSCE	Decision No. 7/17 Strengthening Efforts to Combat all Forms of Child Trafficking	8 December 2017	www.osce.org/files/f/documents/f/b/362016.pdf

National

Bosnia and Herzegovina	2020–2023 Strategy to supress trafficking in human beings in Bosnia and Herzegovina	January 2020	www.msb.gov.ba/PDF/11022020.pdf
United Kingdom	UK's Modern Slavery Strategy 2014	29 November 2014	www.assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/383764/Modern_Slavery_Strategy_FINAL_DEC2015.pdf
United Kingdom	Online Harms White Paper	8 April 2019	www.gov.uk/government/consultations/online-harms-white-paper
United Kingdom	Online Harms White Paper, Full Government Response to Consultation	December 2020	www.assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf

Bibliography

5Rights and Professor Hany Farid, *Briefing: end-to-end encryption and child sexual abuse material* (5Rights Foundation, December 2019).

Agencia Española de Proteccion de Datos, "Canal Prioritario" [website]. Available at: https://www.aepd.es/canalprioritario/ (accessed 21 October 2021).

All-Party Parliamentary Group on Prostitution and the Global Sex Trade, *Behind Closed Doors: Organised sexual exploitation in England and Wales* (APPG, May 2018). Available at: www.appg-cse.uk/wp-content/uploads/2018/05/Behind-closed-doors-APPG-on-Prostitution.pdf (accessed 21 October 2022).

Australian Government eSafetyCommissioner, "*Safety by Design" [website]* (eSafetyCommissioner, 2019). Available at: www.esafety.gov.au/industry/safety-by-design (accessed 21 October 2021).

Baggett, Tony, "Germany is about to block one of the world's biggest porn sites" [website] (Wired, 14 July 2021). Available at: www.wired.co.uk/article/germany-porn-laws-age-checks (accessed 21 October 2021).

Belser, Patrick P., *Forced Labour and Human Trafficking: Estimating the Profits* (Geneva: ILO, March 2005), p. 17. The UN has estimated the total value of human trafficking at US$150 billion.

Better Internet for Kids, "Insafe and INHOPE" [website]. Available at: www.betterinternetforkids.eu/policy/insafe-inhope (accessed 21 October 2021).

Bird Ruiz-Benitez de Lugo, Lucia, *Battling Human Trafficking, A Scrutiny of Private Sector Obligations under the Modern Slavery Act* (Geneva, The Global Initiative against Transnational Organized Crime, April 2018).

Braun, Elisa and Kayali, Laura, "France to introduce controversial age verification system for adult websites" [website] (Politico, 9 July 2020). Available at: www.politico.eu/article/france-to-introduce-controversial-age-verification-system-for-adult-pornography-websites/ (accessed 21 October 2021).

Carter, Mike, "Investigation of FBI's Child Pornography Operation Sparks Controversy Over Internet Privacy" (Government Technology, August 31, 2016).

Cater, Leonie, "How Europe's privacy laws are failing victims of sexual abuse" [website] (Politico, 13 January 2021). Available at: www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/ (accessed 21 October 2021).

Clark, John F., "We Are in Danger of Losing the Global Battle for Child Safety" [website] (NCMEC: 17 November 2020). Available at: www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety (accessed 21 October 2021).

Cole, Samantha, "Sex Workers Say Porn on Google Drive Is Suddenly Disappearing" [website] (Vice, 21 March 2018). Available at: www.vice.com/en/article/9kgwnp/porn-on-google-drive-error (accessed 21 October 2021).

Comey, James B., "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" [website] (FBI, 16 October 2014). Available at: www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed: 21 October 2021).

Committee on the Elimination of Discrimination against Women, *Convention on the Elimination of All Forms of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration* (United Nations, 6 November 2020).

Committee on the Judiciary, "Chairman Graham Applauds Senate Judiciary Committee for Unanimously Approving the EARN IT Act" [website] (US Senate, 2 July 2020). Available at: www.judiciary.senate.gov/press/rep/releases/chairman-graham-applauds-senate-judiciary-committee-for-unanimously-approving-the-earn-it-act (accessed 21 October 2021).

Computer Security Resource Center, *Glossary* [website] (National Institute of Standards and Technology, U.S. Department of Commerce). Available at: www.csrc.nist.gov/glossary/term/cyber security (accessed 21 October 2021).

Council of Europe, "Protocol negotiations of a draft Second Additional Protocol to the Convention on Cybercrime" [website] (Council of Europe). Available at: www.coe.int/en/web/cybercrime/t-cy-drafting-group (accessed 21 October 2021).

Council of Europe, "Reporting on Social Media Platforms" [website] (Council of Europe). Available at:

www.coe.int/en/web/no-hate-campaign/reporting-on-social-media-platforms#{"37117289":[4]} (accessed 21 October 2021).

Council of Europe, Committee on Legal Affairs and Human Rights, *Report 15379 on the Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (Council of Europe, 28 September 2021).

Council of Europe, *Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content* (Lausanne: Council of Europe, January 2017).

Council of Europe, *Convention on Cybercrime* (Budapest: Council of Europe, 23 November 2001).

Council of Europe, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote: Council of Europe, 25 October 2007).

Council of Europe, *Explanatory Report to the Council of Europe Convention on Action against Trafficking in Human Beings* (Warsaw, 16 May 2005).

Council of Europe, *Internet Governance - Council of Europe Strategy 2016-2019* (Council of Europe, September 2016).

Council of Europe, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries* (Council of Ministers, 7 March 2018).

Dart v. Craigslist, Inc., No. 09 C 1385 (N.D. Ill. Oct. 20, 2009). Available at: http://pub.bna.com/eclr/dartvcraigslist.pdf (accessed 21 October 2021).

De Streel, Alexandre et al, *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform* (European Parliament, June 2020).

Deloitte, *2017 Global Mobile Consumer Survey: US edition The dawn of the next era in mobile* (Deloitte, 2017).

Dittrich, Paul-Jasper, *Online Platforms and How To Regulate Them: An EU Overview*, Policy Paper No.227 (Berlin, Jacques Delors Institut, 14 June 2018).

Dr. Hardinghaus, Alexander, Kimmich, Ramona and Schonhofen, Sven, "German government introduces new bill to amend Germany's Hate Speech Act, establishing new requirements for social networks and video-sharing platforms" [website] (Technology Law Dispatch, 6 April 2020). Available at: www.technologylawdispatch.com/2020/04/regulatory/german-government-introduces-new-bill-to-amend-germanys-hate-speech-act-establishing-new-requirements-for-social-networks-and-video-sharing-platforms/ (accessed 21 October 2021).

Dunn, Mark, "Reputational risks are greater than ever for brands associated with slavery" [website] (LexisNexis, 8 October 2019). Available at: www.bis.lexisnexis.co.uk/blog/categories/governance-risk-and-compliance/risks-greater-than-ever-brands-associated-with-slavery (accessed 21 October 2021).

DW, "Germany: Crimes involving child sexual abuse images almost double" [website] (DW, 7 November 2021). Available at: www.p.dw.com/p/42h75 (accessed 20 November 2021).

Dwoskin, Elizabeth and Tiku, Nitasha, "Facebook sent home thousands of human moderators due to the coronavirus. Now the algorithms are in charge" [website] (The Washington Post, 24 March 2020). Available at: www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/ (accessed 21 October 2021).

EUR-Lex, *Communication of the Commission on Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms, COM (2017) 555* (Brussels: Publications Office of the European Union, 28 September 2017).

European Commission, "Alliance to better protect minors online" [website]. Available at: www.digital-strategy.ec.europa.eu/en/policies/protect-minors-online (accessed 21 October 2021).

European Commission, "Fighting child sexual abuse: Commission proposes interim legislation to enable communications services to continue detecting child sexual abuse online" [website] (European Commission, 10 September 2020). Available at: https://digital-strategy.ec.europa.eu/en/news/fighting-child-sexual-abuse-commission-proposes-interim-legislation-enable-communications-services (accessed 21 October 2021).

European Commission, *Commission Staff Working Document. Online Platforms Accompanying the document Communication on Online Platforms and the Digital Single Market. SWD(2016) 172 final* (Brussels, European Commission, 25 May 2016).

European Commission, *Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse* (Brussels: Publications Office of the European Union 24 July 2020).

European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Com-*

mittee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe {SWD(2016) 172 final} (Brussels, European Commission, 25 May 2016).

European Commission, *Cybercrime* [website] (European Commission). Available at: www.ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (accessed 21 October 2021).

European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC* (Official Journal of the European Union, 15 December 2020).

European Parliament and European Council, "*Directive 2011/93/EU 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*" (13 December 2011).

European Parliament and European Council, *Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)* (Official Journal of the European Communities L178/1, 17 July 2000).

European Parliament News, "Detecting online child sexual abuse requires strong safeguards" [website] (European Parliament, 7 December 2020). Available at: www.europarl.europa.eu/news/en/press-room/20201207IPR93202/detecting-online-child-sexual-abuse-requires-strong-safeguards (accessed 21 October 2021).

European Parliament, Council and the Commission, *Inter-institutional Agreement on Better Lawmaking, OJ C 321/01*. (Official Journal of the European Union, 2003).

European Parliament, *REPORT on the Proposal for a Regulation of the European Parliament and of the Council on a Temporary Derogation from Certain Provisions of Directive 2002/58/EC of the European Parliament and of the Council as Regards as the Use of Technologies by Number-Independent Interpersonal Communications Service Providers for the Processing of Personal and Other Data for the Purpose of Combatting Child Sexual Abuse Online* (11 December 2020).

European Parliamentary Research Service, *Liability of Online Platforms* (Brussels: European Parliament, February 2021)

European Tech Alliance, *European Tech Alliance Position on the future eCommerce framework ('Digital Services Act')*, (European Tech Alliance, April 2020).

Europol and Eurojust, *Second report of the observatory function on encryption* (Europol and Eurojust Public Information, 18 February 2020).

Europol, *Catching the virus cybercrime, disinformation and the COVID-19 pandemic* (The Hague: Europol, 3 April 2020).

Europol, *Criminal networks involved in the trafficking and exploitation of underage victims in the European Union* (The Hague: Europol, 18 October 2018).

Europol, *European Union Serious and Organised Crime Threat Assessment. Crime in the age of technology* (The Hague: Europol, 2017).

Facebook Terms of Service. Available at: www.facebook.com/terms.php (accessed 21 October 2021).

Facebook, "Report Something" [website]. Available at: www.facebook.com/help/263149623790594 (accessed 21 October 2021).

Facebook, *NetzDG Transparency Report 2020* [website] (Facebook, July 2020). Available at: www.about.fb.com/wp-content/uploads/2020/07/facebook_netzdg_July_2020_English.pdf (accessed 21 October 2021).

Federal Parliament of Germany, *Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)* (12 July 2017). Available at: www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 21 October 2021).

Federal Parliament of Germany, *German Code of Criminal Procedure as published on 7 April 1987* (Federal Law Gazette I, p. 1074, 1319).

Federal Parliament of Germany, German Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322).

Finck, Michèle, *Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy* (*European Law Review,* 20 June 2017). LSE Legal Studies Working Paper No. 15/2017. Available at: www.ssrn.com/abstract=2990043 and www.dx.doi.org/10.2139/ssrn.2990043 (accessed 29 November 2021).

Finklea, Kristin, *Law Enforcement Using and Disclosing Technology Vulnerabilities* (Congressional Research Service, 26 April 2017).

Five Countries Ministerial, *Voluntary Principles to*

Counter Online Child Sexual Exploitation [website] (U.S. DOJ, 5 March 2020). Available at: www.justice.gov/opa/press-release/file/1256061/download (accessed 21 October 2021).

French National Commission on Informatics and Liberty, "The Digital Rights of Minors" [website] (CNIL, 09 June 2021). Available at: www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne (accessed 21 October 2021).

Frosio, Giancarlo F., *The Death of "No Monitoring Obligations": A Story of Untameable Monsters* (JIPITEC, 2017).

Global Initiative Against Transnational Organized Crime, "Presentation by Katie A. Paul, Co-Director of the Antiquities **Traficking** and Heritage Anthropology Research (ATHAR) Project during "Culture in Ruins: The illicit trade in cultural property in North and West Africa", ENACT, 26 November 2020". Available at: www.globalinitiative.net/analysis/culture-in-ruins-the-illicit-trade-in-cultural-property-in-north-and-west-africa/ (accessed 21 October 2021).

Global Initiative Against Transnational Organized Crime, "Research findings from Digital Disruption programme on the Illegal Wildlife Trade" [website] (GITOC, 05 October 2018). Available at: www.globalinitiative.net/initiatives/digital-dangers/ (accessed 21 October 2021).

Global Initiative Against Transnational Organized Crime, *Preventing Vulnerability of and Strengthening Policy Responses For Commercial Sexual Exploitation Of Children In The Western Balkans* (working title), forthcoming.

Goodman, Marc D. and Brenner, Susan W., "The Emerging Consensus on Criminal Conduct in Cyberspace" (*International Journal of Law and Information Technology* 10/2, 2002).

Google, "Abuse Program Policies and Enforcement" [website] Available at: www.support.google.com/docs/answer/148505?hl=en (accessed 21 October 2021).

Google, "Removals under the Network Enforcement Law" [website]. Available at: https://transparencyreport.google.com/netzdg/youtube?hl=en (accessed 21 October 2021).

Grant, Harriet, "Urgent action needed as rise in porn site traffic raises abuse fears" [website] (The Guardian, 25 March 2020). Available at: www.theguardian.com/global-development/2020/mar/25/urgent-action-needed-as-spike-in-porn-site-traffic-raises-abuse-fears-say-mps (accesses 21 October 2021).

Greijer, Susanna and Doek, Jaap, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (Luxembourg: ECPAT International, June 2016), p. 40. Available at: www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology (accessed 29 November 2021).

GRETA, *Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Germany* (20 June 2019). Available at: www.rm.coe.int/greta-2019-07-fgr-deu-en/1680950011 (accessed 29 November 2021).

Heldt, Amélie, "Reading between the lines and the numbers: an analysis of the first NetzDG reports" *Internet Policy Review Volume 8 Issues 2* [website] (12 June 2019). Available at: www.policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports (accessed 21 October 2021).

Hoang, Thi, "The dual law of technology in trafficking" [website] (The Global Initiative Against Transnational Organized Crime, 23 July 2020). Available at: www.globalinitiative.net/analysis/leveraging-innovation-to-fight-trafficking-in-human-beings-a-comprehensive-analysis-of-technology-tools/ (accessed 21 October 2021).

Human Rights Watch, "COVID-19 and children's rights" [website] (Human Rights Watch, 9 April 2020). Available at: www.hrw.org/news/2020/04/09/covid-19-and-childrens-rights-0#_Toc3725653 (accessed 21 October 2021).

Husovec, Martin and Leenes, Ronald, Tilburg Institute for Law, Technology and Society, *Study on Role of online intermediaries: Summary of the public consultation* (Luxembourg, Publications Office of the European Union, 2014).

ICO, "Introduction to the Age appropriate design code" [website]. Available at: www.ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ (accessed 21 October 2021).

ILO, *Profits and Poverty: The Economics of Forced Labour* (Geneva: ILO, 20 May 2014).

InfoCuria Case-law, *Eva Glawischnig-Piesczek vs. Facebook Ireland Limited, October 2019, Case C-18/18* (Court of Justice of the EU, October 2019). Available at: www.curia.europa.eu/juris/document/document.jsf?docid=218621&doclang=EN (accessed 21 October 2021).

Internet Watch Foundation, *Annual Report 2019* (IWF, 2019).

IOM, *Study Report Exploring the Role of ICTs in Recruitment for Human Trafficking in the Republic of Kazakhstan, the Kyrgyz Republic and the Republic of Tajikistan* (Astana: IOM, 2019).

Keller, Michael H. and Dance, Gabriel J.X., "The internet is overrun with images of child sexual abuse. What went wrong?" [website] (*The New York Times*, 29 September 2019). Available at: www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html (accessed 21 October 2021).

Kessler, Glen, "Has the sex-trafficking law eliminated 90 percent of sex-trafficking ads?" [website] (*The Washington Post,* 20 August 2018). Available at: www.washingtonpost.com/politics/2018/08/20/has-sex-trafficking-law-eliminated-percent-sex-trafficking-ads/ (accessed 21 October 2021).

Knesset of Israel, "*Law on Authorities for the Prevention of Committing Crimes through Use of an Internet Site, 5777-2017*" (Law on Authorities). Available at: www.fs.knesset.gov.il/20/law/20_lsr_390328.pdf (accessed 21 October 2021).

Kranzberg, Melvin, "Technology and History: Kranzberg's Laws," *Technology and Culture 27.3* (Bulletin of Science, Technology and Society, 1 February 1995).

Kristof, Nicholas, "The Children of Pornhub" [website] (*The New York Times*, 4 December 2020). Available at: www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html (accessed 21 October 2021).

Kuczerawy, Aleksandra, "From 'Notice and Take Down' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression", in: Giancarlo Frosio (ed.), *The Oxford Handbook of Intermediary Liability Online* (Oxford: Oxford University Press, 2020).

Langford, Cameron, "Texas Court Refuses to Toss Sex-Trafficking Claims Against Facebook" [website] (Courthouse News Service, 28 April 20200. Available at: www.courthousenews.com/texas-court-refuses-to-toss-sex-trafficking-claims-against-facebook/ (accessed 21 October 2021).

Limer, Eric, "Microsoft to ban "offensive language" from Skype" [website] (Popular Mechanics, 26 March 2018). Available at: www.popularmechanics.com/technology/apps/a19597085/microsoft-service-agreement-offensive-language/ (accessed 21 October 2021).

Lomba, Niombo and Evas, Tatjana, *Digital services act: European added value assessment* (European Parliamentary Research Services, October 2020).

Lovells, Hogan and Forrai, Zachary, "A new era for Australian online safety regulation" [website] (JD Supra, 2 August 2021). Available at: www.jdsupra.com/legalnews/a-new-era-for-australian-online-safety-4740569/ (accessed 21 October 2021).

Marsden, Christopher, *Internet Co-Regulation* (Cambridge University Press 2011).

Martens, Bertin, *An Economic Policy Perspective on Online Platforms. Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05* (European Commission, 2016).

Mello, Gabriela, "Brazil court slashes fine for Facebook's refusal to share WhatsApp data" [website] (Reuters, 25 June 2019). Available at: www.reuters.com/article/us-facebook-fine-brazil/brazil-court-slashes-fine-for-facebooks-refusal-to-share- whatsapp-data-idUSKCN1TQ2RI (accessed 21 October 2021).

Microsoft, Microsoft Services Agreement. Available at: www.microsoft.com/en-us/servicesagreement/default.aspx (accessed 21 October 2021).

Milmo, Dan, "2021 was worst year on record for online child sexual abuse, says IWF" [website] (The Guardian, 13 January 2022). Available at: https://www.theguardian.com/society/2022/jan/13/2021-was-worst-year-on-record-for-online-child-sex-abuse-says-iwf (accessed 25 January 2022).

Ministry of Internal Affairs of Moldova, *Information on the protection of children's rights in the Republic of Moldova on the theme "Information and communications technology and child sexual exploitation" pursuant to Human Rights Resolution 28/19 on the rights of the child*. Available at: www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj0uYexmLb0AhWIM-wKHW6ADSAQFnoECAsQAQ&url=https%3A%2F%2Fohchr.org%2FDocuments%2FIssues%2FChildren%2Fcommunications_technology%2FRepublicofMoldova.docx&usg=AOvVaw2iDSv9i9SWiujI8c-KPfki (accessed 21 October 2021).

Ministry of Investments and Development of Kazakhstan, Resolution No. 60 of 25 January 2016 on the approval of the Regulations of co-operation of State authorities on compliance with the legislation of the Republic of Kazakhstan in the sphere of telecommunications, referring to The Law on Mass Media.

Morrish, Lydia, "The rights of UK sex workers are under threat – why? Everything you need to know" [website] (Huckmag, 21 November 2018). Available at: www.huckmag.com/perspectives/reportage-2/the-rights-of-uk-sex-workers-are-under-threat-why/ (accessed 21 October 2021).

Murgia, Madhumita and Coulter, Martin, "Big Tech attacks UK plan to hold firms liable for harmful content" [website] (*Financial Times*, 1 July 2019). Available at: www.ft.com/content/3de70dd4-99ba-11e9-8cfb-30c211dcd229 (accessed 21 October 2021).

National Criminal Investigation Service (NCIS) of Norway, *Human Trafficking in Norway — Criminal Actors: A Situational Picture Based on Police Sources* (Oslo: NCIS, 20 December 2017).

NCMEC, "Is Your Explicit Content Out There?" [website]. Available at: www.missingkids.org/gethelpnow/isyourexplicitcontentoutthere (accessed 21 October 2021).

NCMEC, *2020 Reports by Electronic Service Providers (ESPs)* [website]. Available at: www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf (accessed 21 October 2021).

NetClean, "What Happens To The Consumption Of Child Sexual Abuse Material When Millions Of People Work From Home?" [website] (NetClean, 3 April 2020). Available at: www.netclean.com/2020/04/03/what-happens-to-the-consumption-of-child-sexual-abuse-material-when-millions-of-people-work-from-home/ (accessed 21 October 2021).

New York State Office of the Attorney General, "A.G. Schneiderman's „Operation: Game Over" Purges Thousands Of Sex Offenders From Online Video Game Networks" [website] (Office of the NY Attorney General, 5 April 2012). Available at: https://ag.ny.gov/press-release/2012/ag-schneidermans-operation-game-over-purges-thousands-sex-offenders-online-video (accessed 21 October 2021).

OECD, *An Introduction to Online Platforms and their Role in the Digital Transformation* (OECD, 13 May 2019).

OECD, *Practical Actions for Companies to Identify and Address the Worst Forms of Child Labour in the Minerals Supply Chains* (Geneva: OECD, 2017).

OSCE and Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools* (Vienna: OSCE and TAT, 22 June 2020).

OSCE, "Statement by Ambassador Petra Schneebauer, National Co-ordinator for Combating Trafficking in Human Beings, Austria, 19th Alliance against Trafficking in Persons: Panel 1" [website] (Vienna: OSCE, 18 April 2019). Available at: www.osce.org/cthb/419933 (accessed 21 October 2021).

OSCE, "Statement by Halla Gunnarsdóttir, Special Adviser on Gender Equality, Iceland, 19th Alliance against Trafficking in Persons: Panel 4" [website] (Vienna: OSCE, 18 April 2019). Available at: www.osce.org/cthb/420167 (accessed 21 October 2021).

OSCE, "Statement by Petya Nestorova, Executive Secretary of the Council of Europe Convention on Action against Trafficking in Human Beings", 19th Alliance against Trafficking in Persons: Panel 4 [website] (Vienna: OSCE, 18 April 2019). Available at: www.osce.org/cthb/420167 (accessed 21 October 2021).

OSCE, *Decision No. 1107 Addendum to the OSCE Action Plan on Combating Trafficking in Human Beings* (Vienna: OSCE, 6 December 2013).

OSCE, UN.GIFT, *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime* (Vienna: OSR-CTHB, UN.GIFT, May 2010).

OSCE/ODIHR and UN Women, *Guidance Addressing Emerging Human Trafficking Trends and Consequences of the COVID-19 Pandemic* (Warsaw: OSCE, 30 July 2020).

Parker, C., "Meta-Regulation: Legal Accountability for Corporate Social Responsibility". In: D. McBarnet, A. Voiculescu, T. Campbell (eds.), *The New Corporate Accountability*, pp. 207–237 (Cambridge University Press, 2007).

Parliament of Albania, Criminal Procedure Code of the Republic of Albania, No. 7905, 21 March 1995.

Parliament of Australia, *Online Safety Act 2021 No. 76, 2021*. Available at: www.legislation.gov.au/Details/C2021A00076 (Accessed 21 October 2021).

Parliament of Estonia, Information Society Services Act, RT I 2004, 29, 191, 14 April 2004.

Parliament of Moldova, Criminal Code of the Republic of Moldova, Nr. 986, 18 April 2002.

Parliament of Moldova, Law of the Republic of Moldova on preventing and combating cybercrime, No. 20, 3 February 2009.

Pepper, Carolyn E., "Monitoring online content: the impact of Eva Glawischnig-Piesczek v Facebook Ireland Limited" [website] (ReedSmith, 12 November 2019). Available at: www.reedsmith.com/en/perspectives/2019/11/monitoring-online-content-the-impact-of-eva-glawischnig-piesczek-v-facebook (accessed 21 October 2021).

PermessoNegato, *State of Revenge* (November 2020). Available at: www.permessonegato.it/doc/PermessoNegato_StateofRevenge_202011.pdf (accessed 21 October 2021).

Pfefferkorn, Riana, "House Introduces Earn It Act Companion Bill, Somehow Manages to Make it Even Worse" [website] (Stanford Law School, the Center for Internet and Society, 5 October 2020). Available at: www.cyberlaw.stanford.edu/blog/2020/10/house-introduces-earn-it-act-companion-bill-somehow-manages-make-it-even-worse (accessed 21 October 2021).

Reeves, Elizabeth and Vibert, Simone, *Access denied: How end-to-end encryption threatens children's safety online* (Children's Commissioner for England, December 2020).

Richey, Valiant, OSCE, "Opinion: Invisible crimes like human trafficking rise during COVID-19" [website] (Thomson Reuters Foundation News, 16 December 2020). Available at: www.news.trust.org/item/20201216122708-84btm (accessed 21 October 2021).

Royal Decree of Spain, Criminal Procedure Law of Spain September 14, 1882.

Rusakova, Mayya M., *Study Report. Exploring the Role of ICTs in Recruitment for Human Trafficking in the Republic of Kazakhstan, the Kyrgyz Republic and the Republic of Tajikistan* (International Organization for Migration, 2019).

Scheck, Justin, Purnell, Newley and Horwitz, Jeff, "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show." [website] (WSJ, 16 September 2021). Available at: www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953?mod=article_inline (accessed 25 January 2021).

Scottish Parliament, Cross-Party Group on Commercial Sexual Exploitation, *Online Pimping: Inquiry Findings Launched* [website] (CPGCSE, 19 March 2021). Available at: www.cpg-cse.com/post/inquirylaunch (accessed 21 October 2021).

Sen, Roop and Chatterjee, Uma, "Lockdown provokes bad memories for trafficking victims" [website] (rediff.com, 18 April 2020). Available at: www.rediff.com/news/column/how-trafficking-victims-dealwith-the-lockdown/20200418.htm (accessed 21 October 2021).

Simmons + Simmons, "Pioneering Dutch Computer Crime Act III entered into force" [website] (Simmons + Simmons, 1 March 2019). Available at: www.simmons-simmons.com/en/publications/ck0bi70lg7kew0b94qi4inld1/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force (accessed 21 October 2021).

Škorvánek, Ivan, Koops, Bert-Jaap, Clayton Newell, Bryce, and Robert, Andrew, *"My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking* (Tilburg Institute For Law, Technology, And Society, 1 April 2019).

Snapchat, "Information for Law enforcement" [website]. Available at: www.snap.com/en-US/safety/safety-enforcement (accessed 21 October 2021). In-app notifications for Snapchat require the user to hold down on the relevant material before the notification option appears.

Spectre, Rob, Childsafe.AI, *Beyond Backpage: Buying and Selling Sex in the United States One Year Later* (Childsafe.ai, 2019).

Spiegel, Johanna, "Germany's Network Enforcement Act and its impact on social networks" [website] (Taylor Wessing, August 2018). Available at: www.taylorwessing.com/download/article-germany-nfa-impact-social.html (accessed 21 October 2021).

Tech Against Trafficking, "The effect of COVID-19: Five impacts on human trafficking" [website] (Tech Against Trafficking, 16 April 2020). Available at: www.techagainsttrafficking.org/the-effect-of-covid-19-five-impacts-on-human-trafficking/ (accessed 21 October 2021).

Telephone interview with Dani Pinter, Senior Legal Counsel at the Law Center of the US National Center on Sexual Exploitation, 8 December 2020.

Telephone interview with Jessica Harrison, Operations Manager, Modern Slavery and Human Trafficking Unit, 19 November 2020.

The Technology Coalition [website]. Available at: www.technologycoalition.org/ (accessed 21 October 2021).

Thorn and Benenson Strategy Group, *Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking. Findings from 2020 quantitative research among 9–17 year olds* (Thorn, May 20219).

Thorn and Bouche, Vanessa, *Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking* (Los Angeles: Thorn, January 2018).

Tinder, "Age verify to chat with matches" [website] (Tinder). Available at: www.help.tinder.com/hc/en-us/articles/360041821872-Age-verify-to-chat-with-matches (accessed 21 October 2021).

Tung, Liz, "FOSTA-SESTA was supposed to thwart sex trafficking. Instead, it's sparked a movement" [website] (WHYY, 10 July 2020). Available at: www.whyy.org/segments/fosta-sesta-was-supposed-to-thwart-sex-trafficking-instead-its-sparked-a-movement/ (accessed 21 October 2021).

U.S. Attorney's Office, Northern District of Texas, "United States v. Wilhan Martono (CityXGuide) Case No. 3:20-CR-00274-N" [website] (USDOJ, 26 October 2021). Available at: www.justice.gov/usao-ndtx/united-states-v-wilhan-martono-cityx-guide (accessed 29 November 2021).

U.S. Department of Justice, Office of Public Affairs, "Backpage's Co-founder and CEO, as well as Several Backpage-Related Corporate Entities, Enter Guilty Pleas" [website] (U.S. Department of Justice, 12 April 2018). Available at: www.justice.gov/opa/pr/backpage-s-co-founder-and-ceo-well-several-backpage-related-corporate-entities-enter-guilty (accessed 21 October 2020).

UK Department for Digital, Culture, Media and Sport, "Statutory guidance. Code of Practice for providers of online social media platforms" [website] (UK Government, 12 April 2019). Available at: www.gov.uk/government/publications/code-of-practice-for-providers-of-online-social-media-platforms/code-of-practice-for-providers-of-online-social-media-platforms (accessed 21 October 2021).

UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper* (UK Government, 8 April 2019).

UK Government, Department for Digital, Culture, Media & Sport and Home Office, *Online Harms White Paper: Full Government Response to the consultation* (UK Government, December 2020).

UK Government, Department for Digital, Culture, Media & Sport and Home Office, *The Government Report on Transparency Reporting in relation to Online Harms* [website] (UK Government, 15 December 2020). Available at: www.assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944320/The_Government_Report_on_Transparency_Reporting_in_relation_to_Online_Harms.pdf (accessed 21 October 2021).

UK National Crime Agency, "NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation" [website] (NCA, 2 July 2020). Available at: www.nationalcrimeagency.gov.uk/news/operation-venetic (accessed 21 October 2021).

UK Parliament, *Draft Online Safety Bill*.

UN News, "Children vulnerable to abuse and violence during coronavirus lockdowns, UN experts warn" [website] (United Nations, 7 April 2020). Available at: www.news.un.org/en/story/2020/04/1061282 (accessed 21 October 2021).

UNODC Commission on Crime Prevention and Criminal Justice, *Resolution 27/2, "Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies"* (Vienna: UNODC, 14–18 May 2018).

UNODC, "E4J University Module Series: Cybercrime, Module 12: Interpersonal Cybercrime. Online child sexual exploitation and abuse" [website] (UNODC, February 2020). Available at: www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html (accessed 21 October 2021).

UNODC, "Transnational organized crime facilitated through technology: the Phantom Secure case." [website] (UNODC). Available at: www.unodc.org/unodc/en/untoc20/truecrimestories/phantom-secure.html (accessed 21 October 2021).

UNODC, Ad hoc committee established by General Assembly resolution 74/247 [website] (UNODC). Available at: www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed: 21 October 2021).

UNODC, *Comprehensive Study on Cybercrime, Draft* (New York: United Nations, 2013).

UNODC, *Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, "Comments received in accordance with the Chair's proposal for the work plan for the period 2018-2021"* (UNODC, 16 March 2018).

US Congress, *H.R.1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017* (Washington: U.S. Government Publishing Office, 4 November 2018).

US Congress, *S.3398 - A bill to establish a National Commission on Online Child Sexual Exploitation Prevention, and for other purposes*. Available at: www.congress.gov/bill/116th-congress/senate-bill/3398/text (accessed 21 October 2021).

US Congress, S.3398 – Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 or the EARN IT Act of 2020.

US Congress, US Communications Decency Act, 47 U.S.C. §230.

US Criminal Code, 18 US C 2258A "Reporting Requirements of Providers", which requires providers to report CSE material to the National Center for Missing and Exploited Children.

US Department of Justice, "International Statement: End-To-End Encryption and Public Safety" [web-

site] (US DOJ Office of Public Affairs, 11 October 2020). Available at: www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety (accessed 21 October 2021).

US Department of Justice, "Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse" [website] (the United States Department of Justice). Available at www.justice.gov/opa/press-release/file/1256061/download (accessed 21 October 2021).

US District Court, Northern District of California, Case No. 3:21-cv-00485-JCS John Doe #1 and John Doe #2 vs. Twitter, Inc. (04 July 2021). Available at: www.endsexualexploitation.org/wp-content/uploads/Doe-v-Twitter_1stAmndComplaint_Filed_040721.pdf (accessed 21 October 2021).

US Federal Bureau of Investigations, "School closings due to COVID-19 present potential for increased risk of child exploitation" [website] (Washington D.C.: FBI, 23 March 2020). Available at: www.fbi.gov/news/pressrel/press-releases/school-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation?utm_campaign=email-Immediate&utm_medium=email&utm_source=national-press-releases&utm_content=%5B795639%5D-%2Fnews%2Fpressrel%2Fpress-releases%2Fschool-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation (accessed 21 October 2021).

US Senate Bill 20. Available at: www.capitol.texas.gov/tlodocs/86R/billtext/pdf/SB00020F.pdf#navpanes=0 (accessed 29 November 2021).

US Senate, Survivors of Human Trafficking Fight Back Act of 2020.

Wager, Livia and Hoang, Thi, *Aggravating circumstances: How coronavirus impacts human trafficking* (Global Initiative against Transnational Organized Crime, May 2020).

Walker, Summer, *Cyber-insecurities? A guide to the UN cybercrime debate* (Geneva, Global Initiative against Transnational Organized Crime, 4 March 2019).

WeProtect Global Alliance, "European Electronic Communications Code briefing" [website] (WeProtect Global Alliance, 16 December 2020). Available at: https://www.weprotect.org/library/european-electronic-communications-code-briefing/ (accessed 21 October 2021).

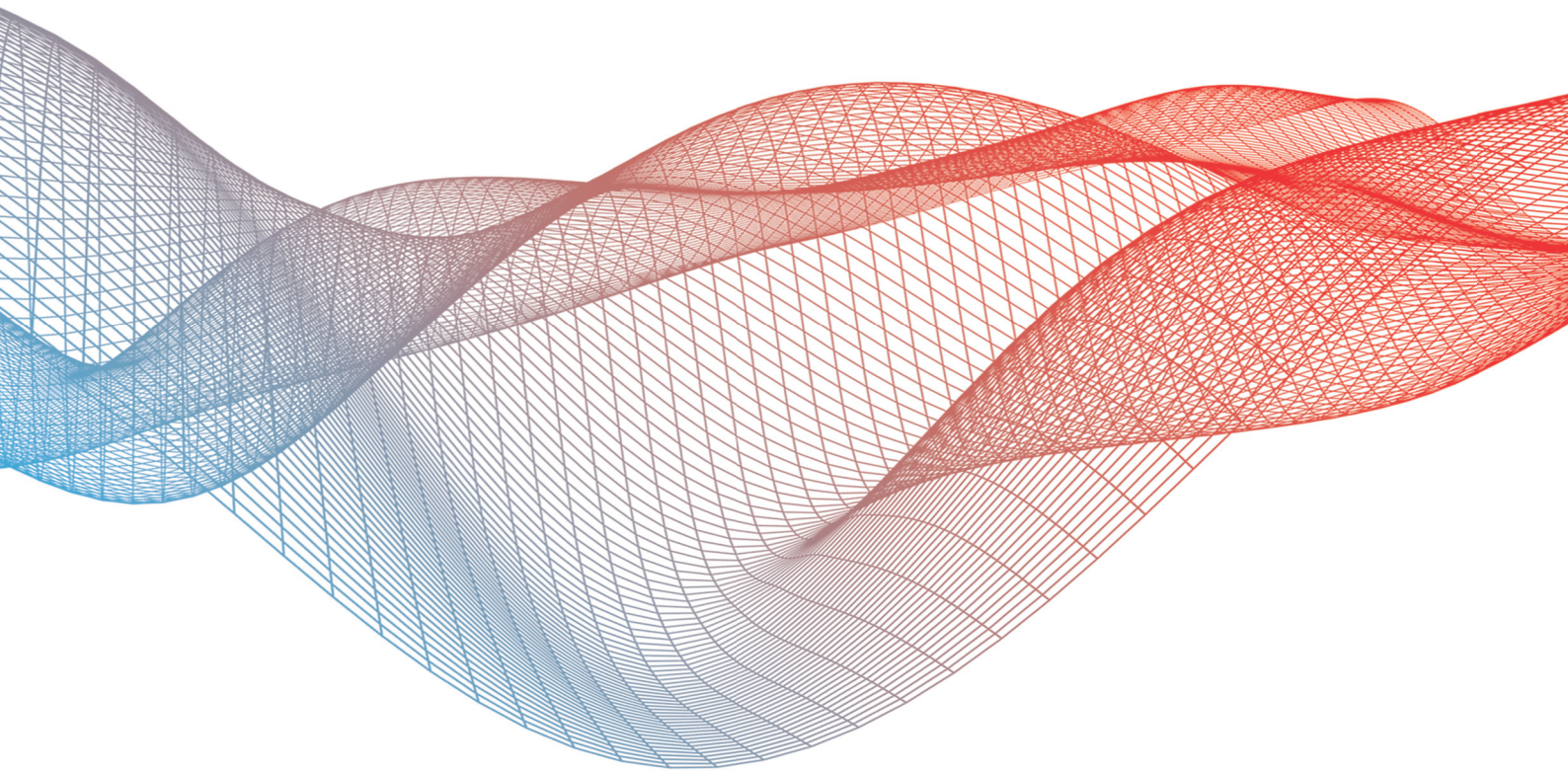
Whitcomb, Dan, "Exclusive: Report gives glimpse into murky world of U.S. prostitution in post-Backpage era" [website] (Reuters, 11 April 2019). Available at: www.reuters.com/article/us-usa-prostitution-internet-exclusive-idUSKCN1RN13E (accessed 29 November 2021).

Written contribution by the competent authorities of Montenegro, 06 October 2020.

Written submission by the Ministry of Justice of Georgia, 28 October 2020.

Written submissions by Anu Leps, National Coordinator against Trafficking in Human Beings, Ministry of Justice, Estonia, 09 October 2020.

Zuckerberg, Mark, "A Privacy-Focused Vision for Social Networking" [website] (Facebook, 6 March 2019). Available at: Available at: www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634 (accessed 21 October 2021).



OSCE Secretariat
Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings
Wallnerstrasse 6
A-1010 Vienna, Austria

E-mail: info-cthb@osce.org

OSCE Organization for Security and Co-operation in Europe