



**UNODC**

United Nations Office on Drugs and Crime

# POLICYMAKING AND THE ROLE OF **ONLINE** **INTERMEDIARIES**

IN PREVENTING AND COMBATING ILLICIT TRAFFICKING





UNITED NATIONS OFFICE ON DRUGS AND CRIME

# ISSUE PAPER

## POLICYMAKING AND THE ROLE OF ONLINE INTERMEDIARIES IN PREVENTING AND COMBATING ILLICIT TRAFFICKING



UNITED NATIONS  
Vienna, 2021

## ACKNOWLEDGEMENTS

This issue paper was prepared under the UNODC Global Programme on Implementing the Organized Crime Convention (Organized Crime and Illicit Trafficking Branch, Division for Treaty Affairs).

### Research and drafting

Lisa Armberger, Colin Craig, Antonio De Vivo, Joe McNamee, Riikka Puttonen

Many individuals and organizations contributed to the preparation of this issue paper. The United Nations Office on Drugs and Crime (UNODC) extends its appreciation to all those who contributed through participation in an Expert Group Meeting held from 4 to 6 February 2020 and/or through the submission of written feedback on drafts of this issue paper. UNODC acknowledges the contribution of the following individuals and organizations:

Mohammad Shadi Alhakeem (NAUSS), Talal Al Mannaei (United Arab Emirates), Ahmed Saleh Mohamed Alzarouni (United Arab Emirates), Kirk Arthur (Microsoft), Victoria Baines (Bournemouth University), Antonio Balsamo (Italy), Tuna Bozalan (UNODC), Cormac Callanan (Aconite Internet Solutions), Celso Coracini (UNODC), Tim Engelhardt (OHCHR), Silvia Galimberti (UNODC), Andreas Gruber (ISPA), Akira Irie (Japan), Fumio Ito (UNODC), Ephraim Percy Kenianito (ARTICLE 19), Alexandra Klosinska (OSCE), Julia Krüger (Netropolitik), Stephen McGlynn (Australia), Eliška Pirková (Access Now), Maximilian Schubert (EuroISPA), Carlos Affonso Souza (ITS Rio), Daoming Zhang (INTERPOL).

© United Nations, September 2021.

The designations employed and the presentation of material in this information product do not imply the expression of any opinion whatsoever on the part of the United Nations Office on Drugs and Crime (UNODC) concerning the legal or development status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The contents of this publication do not necessarily reflect the views or policies of UNODC, Member States or contributory organizations, and neither do they imply any endorsement.

UNODC encourages the use, reproduction and dissemination of material in this information product. Except where otherwise indicated, material may be copied, downloaded and printed for private study, research and teaching purposes, or for use in non-commercial products or services, provided that appropriate acknowledgement of UNODC as the source and copyright holder is given and that endorsement by UNODC of users' views, products or services is not implied in any way.

Cover images: top: ©stock.adobe.com/Johan Swanepoel; middle: ©stock.adobe.com/Pavel Kubarkov; bottom left: ©stock.adobe.com/Andreas Hiekel, FBAS ENTERTAINMENT; bottom right: ©stock.adobe.com/issaronow

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

---

# CONTENTS

INTRODUCTION .....	1
Scope of this paper .....	1
Legal framework .....	2
Structure of this paper .....	3
1. STATEMENT OF THE PROBLEM .....	5
Wildlife crime .....	5
Wildlife crime online .....	6
Falsified medical products .....	7
Falsified medical products online .....	8
Trafficking in cultural property .....	9
Trafficking in cultural property online .....	9
Conclusion .....	11
2. THE INTERNET AND ONLINE INTERMEDIARIES .....	13
What is the Internet? .....	13
What is an online intermediary? .....	15
Internet access providers .....	16
Hosting providers .....	17
Social media providers .....	17
Cloud storage and cloud software providers .....	17
Domain name registrars .....	18
Domain name registry operators .....	18
Search engine providers .....	18
Instant messaging service providers .....	19
Payment service providers .....	19
Cryptocurrency-related service providers .....	19
Relations between online intermediaries and their users .....	20
Conclusion .....	21

3.	STAKEHOLDERS AND THEIR INTERESTS .....	23
	The public .....	23
	Individuals .....	23
	Businesses .....	24
	Online intermediaries .....	24
	Conclusion .....	27
4.	POLICY MEASURES FOR ADDRESSING SELECTED TYPES OF CRIME COMMITTED THROUGH ONLINE INTERMEDIARIES .....	29
	Cooperation-based measures .....	30
	Liability-based measures .....	35
	Liability rules .....	36
	Non-liability rules .....	43
	Issues common to cooperation- and liability-based approaches .....	62
	Jurisdiction .....	62
	Terms of service-based removal of content and withdrawal of services .....	64
	Monitoring, evaluating and adapting measures and the need for transparency .....	66
	Conclusion .....	68
5.	HUMAN RIGHTS .....	71
	Rights implicated by wildlife crime, falsified medical products-related crime and trafficking in cultural property .....	73
	Rights to health and to life .....	73
	Right to take part in cultural life .....	74
	Rights implicated by policy measures addressing wildlife crime, falsified medical products-related crime and trafficking in cultural property online .....	74
	Freedom of expression .....	75
	Right of peaceful assembly .....	76
	Right to privacy .....	77
	Right to effective remedy .....	78
	Permissible restrictions to human rights .....	78
	Conclusion .....	80
	CONCLUSION .....	83



---

# INTRODUCTION

More and more of our lives is taking place online. Today we use the Internet to connect with friends and family, to work, study, organize, communicate and shop. The COVID-19 pandemic, during which this paper was written and published, has starkly demonstrated the importance of the Internet to each of these activities and more. Our connections to each other via the Internet are facilitated by a complex chain of online intermediaries who provide the services that bring us together. These include Internet access providers, hosting service providers, social media services and payment service providers, to name but a few. As society moves online, organized crime is also increasingly taking place online. Organized criminal groups are using a variety of online intermediaries to traffic a wide range of illicit goods.

This issue paper considers the question, from the perspective of State policymaking, of the role of online intermediaries in preventing and combating three forms of serious crime online: wildlife crime, falsified medical products-related crime, and trafficking in cultural property.

Policymaking in this area is complex. For States to effectively prevent and combat these crimes, they must understand key stakeholders in the online ecosystem, the interests of these key stakeholders, how these interests may be affected by various policy measures, and the obligations of States under international human rights law.

In considering the question of the role of online intermediaries in preventing and combating these crimes online, the focus of this paper is not on the small number of rogue online intermediaries that provide their services with the specific intention of facilitating illegal activity but rather the vast majority of online intermediaries that have no intention to commit or facilitate serious crime and would like to assist in preventing and combating such crime where this can be done in a manner that is compatible with the achievement of their commercial objectives.

This paper provides no ready solutions. Rather, it seeks to map the key stakeholders, interests, issues and considerations relevant to policymakers in developing measures to prevent and combat the commission of these crimes online. The aim of this paper is thus to contribute to a stronger knowledge base for future research and policy discussions.

## SCOPE OF THIS PAPER

This issue paper is specifically concerned with the role of online intermediaries in preventing and combating wildlife crime, falsified medical products-related crime, and trafficking in cultural property. It does not address other forms of illegal or otherwise harmful online activities. Accordingly, this paper should not be taken to set out a framework for policymaking to prevent and combat all crimes committed online.

The decision was made to limit the scope of this paper to these three types of crime for three key reasons. First, it was not possible within the scope of this project to cover all forms of crime committed online. Second, each of the three types of crime selected for this paper is increasingly taking place online but policy discussions as to how to address the online dimensions of these crimes are underdeveloped. Finally, each

crime type is a form of organized crime falling within the mandates of the United Nations Office on Drugs and Crime (UNODC).<sup>1</sup>

While this paper is limited to addressing each of these three types of crime, various topics discussed in this issue paper are of a general nature and may therefore also be useful for policymakers when addressing the commission of other forms of organized crime online. At the same time, care should be taken in applying lessons learned from this paper to issues outside the paper's scope and material differences between types of crime should be adequately taken into consideration.

## LEGAL FRAMEWORK

The legal framework through which this paper examines the role of online intermediaries in preventing and combating wildlife crime, falsified medical products-related crime, and trafficking in cultural property online includes, firstly, the United Nations Convention against Transnational Organized Crime (Organized Crime Convention).<sup>2</sup> As at the date of publication, the Organized Crime Convention has 190 parties – near universal adherence. Article 1 of the Convention states that its purpose is “to promote cooperation to prevent and combat transnational organized crime more effectively”.

The Organized Crime Convention applies to, inter alia, “serious crime” involving an organized criminal group.<sup>3</sup> The Convention defines “serious crime” as conduct constituting an offence punishable by a maximum sentence of at least four years’ imprisonment.<sup>4</sup> Wildlife crime, falsified medical products-related crime, and trafficking in cultural property each entail conduct which may, depending on the specific offences and the domestic legislative framework in question, constitute “serious crime”. In adopting the Organized Crime Convention, the General Assembly stated that it was “strongly convinced that the [Convention] will constitute an effective tool and the necessary legal framework for international cooperation in combating, inter alia, such criminal activities as ... illicit trafficking in endangered species of wild flora and fauna [and] offences against cultural heritage”.<sup>5</sup>

More concretely, article 10 of the Organized Crime Convention requires that States parties establish the liability of legal persons for participation in serious crimes involving an organized criminal group.<sup>6</sup> Such liability may be criminal, civil or administrative. Article 10 constitutes an important recognition of the role that legal persons may play in the commission or facilitation of organized crime. Where online intermediaries with legal personality are themselves involved in the commission of serious crimes involving an organized criminal group, article 10 requires, in effect, that States parties have legislation under which they can be found liable, whether such liability is criminal, civil or administrative. Furthermore, States parties must ensure that legal persons held liable in accordance with article 10 are subject to effective, proportionate and dissuasive sanctions.<sup>7</sup>

In the vast majority of cases, online intermediaries are not themselves involved in the commission of serious crimes, but rather their services are abused by criminals to carry out offences. In such circumstances, cooperation between online intermediaries and law enforcement authorities can be critical. The Organized Crime Convention contemplates a degree of cooperation between law enforcement agencies and

<sup>1</sup> See, for example, resolution 10/5 entitled “Preventing and combating the manufacturing of and trafficking in falsified medical products as forms of transnational organized crime”, resolution 10/6 entitled “Preventing and combating crimes that affect the environment falling within the scope of the United Nations Convention against Transnational Organized Crime” and resolution 10/7 entitled “Combating transnational organized crime against cultural property” (CTOC/COP/2020/10, chap. I).

<sup>2</sup> United Nations, *Treaty Series*, vol. 2225, No. 39574.

<sup>3</sup> Organized Crime Convention, art. 3, para. 1 and art. 5.

<sup>4</sup> *Ibid.*, art. 2 (b).

<sup>5</sup> General Assembly resolution 55/25.

<sup>6</sup> Organized Crime Convention, art. 10, para. 1.

<sup>7</sup> *Ibid.*, art. 10, para. 4.



prosecutors and the private sector in the prevention of organized crime.<sup>8</sup> The Conference of the Parties to the United Nations Convention against Transnational Organized Crime has also encouraged the private sector to strengthen its cooperation and work with States parties to the Organized Crime Convention and the Protocols thereto in order to achieve the full implementation of these instruments.<sup>9</sup>

In addition to the Organized Crime Convention, this paper also examines the role of online intermediaries in preventing and combating serious crime under the framework of international human rights law. International human rights law is of crucial importance to policymaking in this area. States must take into account their duties to respect, protect and fulfil human rights under international human rights law when developing policies to prevent and combat serious crime committed online. In relation to wildlife crime, falsified medical products-related crime and trafficking in cultural property online and the measures taken by States to address those crimes, this includes, inter alia, the right to health, the right to life, the right to take part in cultural life, freedom of expression, the right of peaceful assembly, the right to privacy and the right to effective remedy.

## STRUCTURE OF THIS PAPER

The issue paper is structured as follows. Chapter 1 provides a statement of the problems that this paper is seeking to address. It provides a brief introduction to wildlife crime, falsified medical products-related crime, and trafficking in cultural property, firstly in relation to the nature and scale of these crimes in general and secondly in relation to their commission online.

Chapter 2 provides a short introduction to the Internet. It also offers an overview of the range of online intermediaries that individuals and organizations rely on in order to use the Internet, explaining their respective functions and, based on the intermediaries' functions, how each intermediary is situated to take action against the commission of serious crime online. It further discusses the nature of relations between online intermediaries and their users.

After looking at specific types of intermediaries in chapter 2, chapter 3 provides a more general overview of the stakeholders of online services and assesses the needs of broad stakeholder groups such as individuals, businesses and organizations and intermediaries themselves.

Chapter 4 then looks at the broad types of policy measures that may be taken by States and online intermediaries to address the commission of serious crimes online, with reference to relevant legislative examples from around the world. It first looks at cooperation-based approaches and then liability-based approaches. It then discusses a range of legal and practical issues common to both types of approach.

Chapter 5 examines the human rights implications of the crimes covered by this paper and actions taken by States and online intermediaries to fight these crimes online, with reference to the applicable international human rights law framework.

Finally, this paper draws each of these strands together in its conclusion.

<sup>8</sup> Ibid., art. 31, para. 2 (a).

<sup>9</sup> Resolution 6/1 entitled "Ensuring effective implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto" (CTOC/COP/2012/15, para. 18).



---

# Chapter 1.

## STATEMENT OF THE PROBLEM

Effective policymaking must begin with a clear statement of the problem. Where policy interventions are developed without a clear idea of the problem that they seek to address, they are unlikely to be appropriate or adapted to addressing the problem. Accordingly, this chapter seeks to provide a brief statement of the problems that this paper seeks to contribute to addressing.

This chapter is divided into sections addressing each of the three crime types covered by this paper. Each section first provides an overview of the nature, scale and gravity of the crime in general. Following this, each section then provides an overview of the commission of the crime online. Finally, relevant similarities between each of these types of crime are discussed in the conclusion to the chapter.

### WILDLIFE CRIME

In recent years, the menace of wildlife crime has grown in the public consciousness. The harmful and destructive effects of wildlife crime should not be underestimated. Wildlife crime contributes to the destruction of wildlife resources and ecosystems, desertification, environmental degradation as well as the reduction and extinction of species. It impacts a wide range of wild animal species, including rhinos, elephants, pangolins, tigers, parrots, reptiles and eels, as well as number of plant species, such as the variety of tropical hardwoods commonly referred to as “rosewood”. It also threatens livelihoods, impacts national security, and undermines social and economic development. Least-developed countries are particularly affected by wildlife crime. Additionally, the recent COVID-19 pandemic has highlighted the potential effects of zoonotic diseases on human health. The illicit wildlife trade is one of a number of factors responsible for the spread of such diseases.<sup>10</sup>

Wildlife crime has grown into a significant and specialized area of transnational organized crime.<sup>11</sup> While it is difficult to accurately quantify the scale of wildlife crime, what is clear is that wildlife crime is a multi-billion-dollar industry and one of the most profitable forms of illicit trafficking. The annual gross illicit income generated by ivory reaching South-East and East Asia alone was recently estimated to be \$400 million, with the same figure for rhino horn being approximately \$230 million.<sup>12</sup>

---

<sup>10</sup> *World Wildlife Crime Report: Trafficking in Protected Species* (United Nations publication, 2020) p. 34.

<sup>11</sup> *Ibid.*, p. 109.

<sup>12</sup> *Ibid.*, pp. 117–118.



Data on seizures also give an indication of the scale of the crime. “Operation Thunderball”, a joint operation led by INTERPOL and the World Customs Organization over four weeks in 2019 and involving police and customs administrations in 109 countries led to the seizure of nearly 10,000 live turtles and tortoises and more than 4,300 birds, among other wildlife specimens and products.<sup>13</sup>

The General Assembly has expressed its deep concern about crimes that affect the environment, including wildlife trafficking, and encouraged Member States to adopt effective measures to prevent and counter wildlife trafficking and poaching.<sup>14</sup>

Although the serious threats posed by wildlife crime have become increasingly recognized, there is no universally-accepted definition of wildlife crime; nor are there international instruments that attempt to propound such a definition.<sup>15</sup> For the purposes of this publication, however, wildlife crime may be taken to refer to the harvesting and trade of wild flora and fauna contrary to national law, including but not limited to national laws implementing obligations under the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES).<sup>16</sup>

## Wildlife crime online

While acts such as poaching and illegal harvesting necessarily involve crimes committed offline, wildlife crime continues online when listed or illicitly obtained wildlife specimens and products are trafficked using the Internet. In other cases, wildlife crime is committed online when legally obtained wildlife specimens and products are illicitly trafficked using the Internet. A growing amount of wildlife trade is now occurring online,<sup>17</sup> a fact which has been recognized with concern by the General Assembly.<sup>18</sup>

While online marketplaces continue to be the most popular platforms for wildlife trade online, a growing amount of trade is occurring on social media platforms.<sup>19</sup> Trends of wildlife trafficking increasingly taking place through social media and messaging apps have been observed in relation to a number of wildlife species, such as reptiles and big cats.<sup>20</sup> One study of illicit marketplaces operating in the United Kingdom of Great Britain and Northern Ireland found 1,194 advertisements selling a total of 2,456 specimens at a price of almost \$1 million.<sup>21</sup> In some countries, wildlife traffickers are reported to prefer online sales to physical markets as they entail lower overhead costs and less scrutiny from authorities.<sup>22</sup> Traffickers change usernames and use technologies such as virtual private networks (VPNs) to avoid apprehension.<sup>23</sup> When online sales points are detected by law enforcement authorities, they simply move to different online platforms.<sup>24</sup>

Indications of large-scale trafficking in wildlife specimens online have prompted action by NGOs and certain online intermediaries. In some countries, online intermediaries and NGOs have cooperated extensively to prevent wildlife trafficking online. A notable example is the Coalition to End Wildlife Trafficking Online, a partnership between the World Wildlife Fund (WWF), TRAFFIC, the International Fund for Animal Welfare (IFAW) and a number of global tech companies. The Coalition was launched in 2018 with

<sup>13</sup> International Criminal Police Organization (INTERPOL), “Wildlife trafficking: organized crime hit hard by joint INTERPOL-WCO global enforcement operation”, press release, 10 July 2019.

<sup>14</sup> General Assembly resolutions 75/196, 74/177, 73/343, 73/185 and 71/326. See also resolution 10/6 (CTOC/COP/2020/10).

<sup>15</sup> *World Wildlife Crime Report*, p. 29.

<sup>16</sup> *Ibid.*

<sup>17</sup> *World Wildlife Crime Report*, p. 13.

<sup>18</sup> General Assembly resolution 71/326.

<sup>19</sup> Jo Hastie, “Disrupt: wildlife cybercrime”, Annelyn Close and Clare Sterling, eds. (London, International Fund for Animal Welfare, 2018) p. 30.

<sup>20</sup> *World Wildlife Crime Report*, pp. 13, 15 and 87.

<sup>21</sup> Hastie, “Disrupt: wildlife cybercrime”, p. 42.

<sup>22</sup> *World Wildlife Crime Report*, p. 76.

<sup>23</sup> Coalition to End Wildlife Trafficking Online, “Offline and in the wild: a progress report of the Coalition to End Wildlife Trafficking Online” (2020), p. 3.

<sup>24</sup> *World Wildlife Crime Report*, p. 76.

21 members, a number which grew to 40 in its first three years of operation.<sup>25</sup> The companies in the coalition include major online intermediaries from Africa, Asia, Europe and North America, with a combined total of nine billion user accounts. The Coalition convenes dialogues to share lessons learned and best practices, and the WFF, Traffic and IFAW also provide member companies with trade data, training materials, policy guidance and education information for users.<sup>26</sup>

While cooperation between States and online intermediaries is essential to preventing and combating online wildlife trafficking effectively, there is little research indicating when, if and how such cooperation occurs, the gaps in cooperative efforts and how cooperation can be improved. There is also a lack of data about how actions taken by intermediaries in response to wildlife trafficking actually address the problem. Reports of numbers of listings removed by an intermediary, for example, often obscure the difference between listings removed for illegality and listings removed for simply being contrary to that intermediary's terms of service. In order to properly evaluate the effectiveness of actions taken by online intermediaries to prevent crimes such as wildlife trafficking occurring over their services, it is important for online intermediaries to record such data and publish meaningful transparency reports about these actions.

## FALSIFIED MEDICAL PRODUCTS

Falsified medical products are, according to a definition endorsed by the seventieth World Health Assembly, “[m]edical products that deliberately/fraudulently misrepresent their identity, composition or source.”<sup>27</sup> Medical products are medicines, excipients and active substances, as well as medical devices, their parts and materials, and accessories used in conjunction with medical devices. This definition of falsified medical products excludes any consideration related to intellectual property rights.<sup>28</sup>

Falsified medical products have negative public health, economic and socioeconomic consequences.<sup>29</sup> They may be of poor quality, unsafe or ineffective. They may endanger health, prolong illness, promote antimicrobial resistance and the spread of drug-resistant infection, and kill patients.<sup>30</sup> They may also undermine confidence in health professionals, health-care systems and legitimate medical products, resulting in further negative public health consequences if patients forego treatment or seek alternative treatment from unregulated care providers.<sup>31</sup>

Low- and middle-income countries are the hardest hit by falsified medical products. A 2017 WHO study found that the observed failure rate of substandard and falsified medical products in low- and middle-income countries was approximately 10.5 per cent.<sup>32</sup> The value of this market was estimated at approximately \$30.5 billion.<sup>33</sup>

The dangers posed by falsified medical products have gained increased recognition in recent years. In resolution 10/5 of the Conference of the Parties to the Organized Crime Convention, the Conference expressed its concern regarding falsified medical products as a continuing global issue with severe multidimensional consequences and, inter alia, called upon States parties that had not yet done so to develop and implement,

<sup>25</sup> Ibid., p. 4.

<sup>26</sup> Coalition to End Wildlife Trafficking Online, “About the Coalition”, available at [www.endwildlifetraffickingonline.org/about](http://www.endwildlifetraffickingonline.org/about).

<sup>27</sup> World Health Organization (WHO), Member State mechanism on substandard and falsified medical products” document WHA70/2017/REC/1, decision WHA70(21), endorsing the definitions set out in document A70/23, appendix 3.

<sup>28</sup> WHO, document A70/23, appendix 3, para. 7 (c).

<sup>29</sup> See WHO, *A Study on the Public Health and Socioeconomic Impact of Substandard and Falsified Medical Products* (Geneva, 2017) pp. 15–19; WHO, *WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products* (Geneva, 2017) pp. 5–7. See further, Tim K. Mackey and Gaurvika Nayyar, “A review of existing and emerging digital technologies to combat the global trade in fake medicines”, *Expert Opinion on Drug Safety*, vol. 16, No. 5 (May 2017), p. 587.

<sup>30</sup> WHO, *A Study on the Public Health and Socioeconomic Impact*, pp. 15–16.

<sup>31</sup> Ibid., p. 17.

<sup>32</sup> Ibid., p. 7.

<sup>33</sup> WHO, *WHO Global Surveillance and Monitoring System*, p. 8.

as appropriate, effective and comprehensive legal frameworks to prevent, prosecute and punish the manufacturing of and trafficking in falsified medical products.<sup>34</sup>

The COVID-19 pandemic has further shone a light on the threats posed by falsified medical products.<sup>35</sup> COVID-19 has been the catalyst for the emergence of a heretofore unseen global market for trafficking in falsified personal protective equipment.<sup>36</sup> There is also evidence of trafficking in other forms of falsified medical products purporting to test or treat COVID-19.<sup>37</sup> As potential medicines that may prevent or treat COVID-19 start to emerge, it is anticipated that falsified versions of these products will also emerge, including falsified vaccines.<sup>38</sup>

## Falsified medical products online

Trafficking in falsified medical products takes place both offline and online.<sup>39</sup> Online, trafficking takes place on online marketplaces, online pharmacies, e-commerce platforms and social media, among other platforms.<sup>40</sup> The number of online pharmacies has greatly increased in recent years, as well as the number of people purchasing medical products online.<sup>41</sup> Nevertheless, the majority of online pharmacies “conduct business illegally and without appropriate safeguards, including not requiring a valid prescription, operating without a valid licence/certification, and failing to meet national or international pharmacy regulations”.<sup>42</sup> Online pharmacies pose particular challenges to investigating and prosecuting authorities, including practical difficulties in identifying physical locations and jurisdictional challenges.<sup>43</sup>

Despite the challenges, there are examples of successful law enforcement actions against online trafficking in falsified medical products. The most high-profile action is Operation Pangea, a yearly week of law enforcement and customs action coordinated by INTERPOL targeting the online sale of falsified medicines and medical devices.<sup>44</sup> Operation Pangea was launched in 2008 and has run every year since then. The operation relies on cooperation between law enforcement and customs and a variety of online and offline intermediaries including payment providers, domain name registrars, Internet access providers, social media services and delivery services.<sup>45</sup> In its first eleven years, Operation Pangea involved a total of 153 participating countries and led to the seizure of 1.1 million packages, the arrest of 3,000 people, and 82,000 websites being taken down.<sup>46</sup> In 2020, Operation Pangea XIII saw a rise in falsified medical products related to COVID-19.<sup>47</sup>

The WHO has noted the need for further research into the operations of the range of online platforms and markets selling falsified medical products in order to more effectively regulate these platforms.<sup>48</sup>

<sup>34</sup> CTOC/COP/2020/10, chap. I, resolution 10/5.

<sup>35</sup> See further UNODC, “Research brief on COVID-19-related trafficking of medical products as a threat to public health” (Vienna, 2020).

<sup>36</sup> Ibid., p. 10.

<sup>37</sup> Ibid., p. 9.

<sup>38</sup> Ibid.

<sup>39</sup> See Tim K. Mackey and others, “Counterfeit drug penetration into global legitimate medicine supply chains: a global assessment”, *The American Journal of Tropical Medicine and Hygiene*, vol. 92, No. 6 (Suppl.) (2015).

<sup>40</sup> WHO, “Substandard and falsified medical products”, 31 January 2018; WHO, *WHO Global Surveillance and Monitoring System*, p. 15.

<sup>41</sup> WHO, *WHO Global Surveillance and Monitoring System*, p. 15.

<sup>42</sup> Mackey and Nayyar, “A review of existing and emerging digital technologies”.

<sup>43</sup> WHO, *A Study on the Public Health and Socioeconomic Impact*, p. 22; WHO, *WHO Global Surveillance and Monitoring System*, p. 16.

<sup>44</sup> For further information, see INTERPOL, “Pharmaceutical crime operations”, available at [www.interpol.int/](http://www.interpol.int/).

<sup>45</sup> See INTERPOL, “Illicit online pharmaceuticals: 500 tonnes seized in global operation”, 23 October 2018; INTERPOL, “Global operation strikes at online supply of illegal and counterfeit medicines worldwide”, 29 September 2011; INTERPOL, “International operation targets online supply of counterfeit and illegal medicines”, 14 October 2010.

<sup>46</sup> INTERPOL, “Operation Pangea: shining a light on pharmaceutical crime”, 21 November 2019.

<sup>47</sup> INTERPOL, “Global operation sees a rise in fake medical products related to COVID-19”, 19 March 2020.

<sup>48</sup> WHO, *A Study on the Public Health and Socioeconomic Impact*, p. 22.



## Trafficking in cultural property

Trafficking in cultural property is a crime which harms cultural heritage – the unique testimony to the identity of peoples and humankind.<sup>49</sup> Trafficking in cultural property deprives peoples of fundamental elements of their identity and of valuable resources for their sustainable development, dispossessing them of their past and thus prejudicing their future.

The General Assembly has expressed its alarm “at the growing involvement of organized criminal groups in all forms and aspects of trafficking in cultural property and related offences”<sup>50</sup> and reaffirmed on numerous occasions the need to strengthen international cooperation in preventing, prosecuting and punishing all aspects of trafficking in cultural property.<sup>51</sup>

While trafficking in cultural property is an important problem in its own right, the relationship between this crime and terrorist financing in some regions has increased the urgency of addressing this type of crime. International and regional bodies such as the Security Council and the European Parliament have on numerous occasions expressed their concern about and condemned trafficking in cultural property being used to finance terrorist groups such as ISIS/Daesh in Iraq and the Syrian Arab Republic<sup>52</sup> and terrorist groups in the Sahel region.<sup>53</sup>

Notwithstanding the international consensus concerning the need to prevent and combat trafficking in cultural property, there is no single, universally agreed-upon definition of “cultural property”.<sup>54</sup> Article 1 of the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, adopted by the General Conference of UNESCO in 1970, defines “cultural property”, for the purposes of that convention, as “property which, on religious or secular grounds, is specifically designated by each State as being of importance for archaeology, prehistory, history, literature, art or science” and which falls within specific categories enumerated in that article. Article 2 of the UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects, adopted in 1995, defines “cultural objects” as those objects which “on religious or secular grounds, are of importance for archaeology, prehistory, history, literature, art or science” and which belong to one of the categories listed in the annex to the convention. This definition is similar to that in article 1 of the 1970 UNESCO convention but does not require that such objects be specifically designated by a State as being of importance.

There is also no internationally agreed-upon definition of “trafficking in cultural property”. Trafficking in cultural property is generally understood as a phenomenon rather than a single type of conduct in relation to cultural property.<sup>55</sup> Trafficking hence refers to a broad range of conduct relating to the illicit trade in cultural property.

## Trafficking in cultural property online

The trafficking of cultural property over the Internet has also been recognized as a matter of concern for the international community.<sup>56</sup> The General Assembly, in expressing its alarm at the “growing involvement of

<sup>49</sup> See further International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences (General Assembly resolution 69/196).

<sup>50</sup> Ibid.

<sup>51</sup> General Assembly resolutions 73/130, 69/196 and 66/180. See also CTOC/COP/2020/10, resolution 10/7.

<sup>52</sup> See, for example, Economic and Social Council resolutions 2199 (2015), 2347 (2017) and 2462 (2019); European Parliament resolution of 30 April 2015 on the destruction of cultural sites perpetrated by ISIS/Daesh (*Official Journal of the European Union*, C 346, 21 September 2016).

<sup>53</sup> See, for example, Economic and Social Council resolution 2374 (2019).

<sup>54</sup> United Nations Educational, Scientific and Cultural Organization (UNESCO), International Standards Section, Division of Cultural Heritage, “Legal and practical measures against illicit trafficking in cultural property: UNESCO handbook” (Paris, 2006), p. 4.

<sup>55</sup> UNODC, *Practical Assistance Tool to Assist in the Implementation of the International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences* (Vienna, 2016).

<sup>56</sup> See further, UNESCO, INTERPOL and International Council of Museums, “Basic actions concerning cultural objects being offered for sale over the Internet” (2006).

organized criminal groups in all forms and aspects of trafficking in cultural property and related offences”, has noted that illicitly trafficked cultural property “is increasingly being sold through a multitude of markets, including over the Internet”<sup>57</sup> and urged Member States to take appropriate measures to regulate the online trade in cultural property.<sup>58</sup> In 2018, the Commission on Crime Prevention and Criminal Justice (CCPCJ), the principal policymaking body of the United Nations in the field of crime prevention and criminal justice, called on Member States to “take effective measures to prevent the transfer of illicitly acquired or illegally obtained cultural property, in particular through auctions, including over the Internet”.<sup>59</sup>

Beginning in the late 1990s, as the world witnessed a rapid growth in online commerce, a portion of the world’s illicit trade in cultural property also started to move online.<sup>60</sup> Since the late 2000s, social media and communications apps have also been used by traffickers to conduct trade online.<sup>61</sup> The shift to online trade has expanded the potential customer base for traffickers, created new markets for small, inexpensive objects such as coins that previously would not have been profitable to trade, and provided traffickers with opportunities to sell cultural property and receive payment undetected.<sup>62</sup> This has also led to a rise in the number of dealers in trafficked cultural property.<sup>63</sup> Authorities investigating trafficking in cultural property online face a number of challenges, including the variety of platforms on which cultural property is trafficked online, missing information hindering proper identification of items and their provenance, and difficulties identifying vendors. Traffickers of cultural property operating online have been identified as using technological countermeasures to avoid detection such as IP-address spoofing.<sup>64</sup>

A number of joint international customs and police operations have targeted trafficking in cultural property, including trafficking committed through the Internet. Operations Pandora, beginning in 2016, and Athena, beginning in 2017, have brought together a number of domestic law enforcement agencies and customs authorities, as well as INTERPOL, Europol, the World Customs Organization and UNESCO to target trafficking in cultural property.<sup>65</sup> Operations Athena II and Pandora IV, which ran in 2019, led to the seizure of 19,000 items, including 8,670 cultural objects for online sale, and the arrests of 101 persons.<sup>66</sup>

Several reports have pointed to the need for increased cooperation between online intermediaries and law enforcement agencies to combat trafficking in cultural property online.<sup>67</sup>

<sup>57</sup> General Assembly resolution 69/196. See also General Assembly resolution 66/180 and CTOC/COP/2020/10, resolution 10/7.

<sup>58</sup> General Assembly resolution 73/130, para. 19.

<sup>59</sup> See Official Records of the Economic and Social Council, 2018, Supplement No. 10 (E/2018/30), chap. I, sect. C, resolution 27/5, para. 11.

<sup>60</sup> European Commission, *Illicit Trade in Cultural Goods in Europe: Characteristics, Criminal Justice Responses and An Analysis of the Applicability of Technologies in the Combat against the Trade* (Luxembourg, Publications Office of the European Union, 2019), p. 106; UNESCO, Fourth Session of the Subsidiary Committee of the Meeting of States Parties to the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, document C70/16/4.SC/10, para. 7.

<sup>61</sup> European Commission, *Illicit Trade in Cultural Goods in Europe*, p. 106; UNESCO, document C70/16/4.SC/10, paras. 20–22.

<sup>62</sup> European Commission, *Illicit Trade in Cultural Goods in Europe*, p. 106.

<sup>63</sup> Ibid.

<sup>64</sup> European Commission, *Commission Staff Working Document Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on the Import of Cultural Goods*, SWD(2017) 262 final (Brussels, 2017), p. 15.

<sup>65</sup> INTERPOL, “Creating a national cultural heritage Unit: the value of a national unit dedicated to fighting crimes against cultural heritage and the illicit traffic of cultural property” (January 2019), p. 27; INTERPOL, “Over 41,000 artefacts seized in global operation targeting trafficking of cultural goods”, 21 February 2018; INTERPOL, “More than 18,000 objects seized and 59 arrested in operation targeting cultural goods”, 29 July 2019; INTERPOL, “101 arrested and 19,000 stolen artefacts recovered in international crackdown on art trafficking”, 6 May 2020.

<sup>66</sup> INTERPOL, “101 arrested and 19,000 stolen artefacts recovered”.

<sup>67</sup> See, for example, UNESCO, INTERPOL and International Council of Museums, “Basic actions concerning cultural objects being offered for sale”; UNESCO, *Fighting the Illicit Trafficking of Cultural Property: A Toolkit for European Judiciary and Law Enforcement* (Paris, 2018), p. 81; INTERPOL and others, “Protecting cultural heritage: an imperative for humanity — acting together against destruction and trafficking of cultural property by terrorist and organized crime groups (2016), p. 8.

## CONCLUSION

This chapter has provided a description of the problems that this issue paper seeks to address: wildlife crime, falsified medical products-related crime, and trafficking in cultural property. It has done so by first providing an overview of the nature, scale and gravity of each of these crime types. It has then provided an overview of the commission of each of these crimes online.

In providing an overview of each of these crimes, this chapter has touched on several common features of each of these crimes which may be relevant to developing policies to address them. This conclusion seeks to bring these common features to the fore.

First, by any definition of the word, these crimes are serious. They are serious in terms of the harms that they cause – to health, to life, to the environment, to economies, to security and to cultural heritage. They are serious in terms of their scale. Each of these three types of crime is global in scale, and particularly affect least-developed countries. The value of these illicit markets ranges from several hundreds of millions of dollars to multiple billions of dollars per year. Depending on the criminal legislation of the country in question, each of these three crimes may also constitute “serious crimes” under the definition of the term provided in the Organized Crime Convention and are hence amenable to the application of the Convention’s provisions. Finally, the seriousness of these crimes has been repeatedly recognized by the international community, including through resolutions of the General Assembly, the Security Council, the Conference of the Parties to the Organized Crime Convention and the Commission on Crime Prevention and Criminal Justice.

Secondly, all three forms of crime are crimes that predate the Internet but are increasingly being committed online, including through social media services. Furthermore, trafficking in wildlife products, falsified medical products and cultural property are phenomena which involve offline acts. All three forms of crime generally (but not always) involve crimes being committed offline before the online element of the crime takes place. All three forms of crime involve the trafficking of physical products which cannot be transported, imported, exported, distributed or stored online. Accordingly, addressing the commission of each crime online is not, and cannot be, a complete response to the crime type. If trafficking in wildlife specimens, falsified medical products and cultural property online were to disappear overnight, poaching of wildlife, manufacture of falsified medical products, and looting and illegal excavation of cultural property would persist. Approaches to preventing and combating wildlife crime, falsified medical products-related crime and cultural property crime must also address offline crime, not just online trafficking.

A third similarity between wildlife crime, falsified medical products-related crime and trafficking in cultural property online is that there are analogous licit markets for wildlife products, medical products and cultural property and that it is sometimes difficult to distinguish between instances of licit and illicit trade. This is because trafficked goods may be indistinguishable or difficult to distinguish from licit goods or that the legality or illegality of an act of sale, offering for sale, distribution, transportation, import, export and so on may depend on external circumstances. The difficulty of distinguishing between instances of licit and illicit trade poses particular difficulties for online intermediaries when they are made legally responsible in relation to trafficking that takes place over their services. Where this is the case, online intermediaries are naturally likely to err on the side of overrestricting the use of their services rather than risk exposing themselves to liability for failing to adequately address trafficking over their services.





---

# *Chapter 2.*

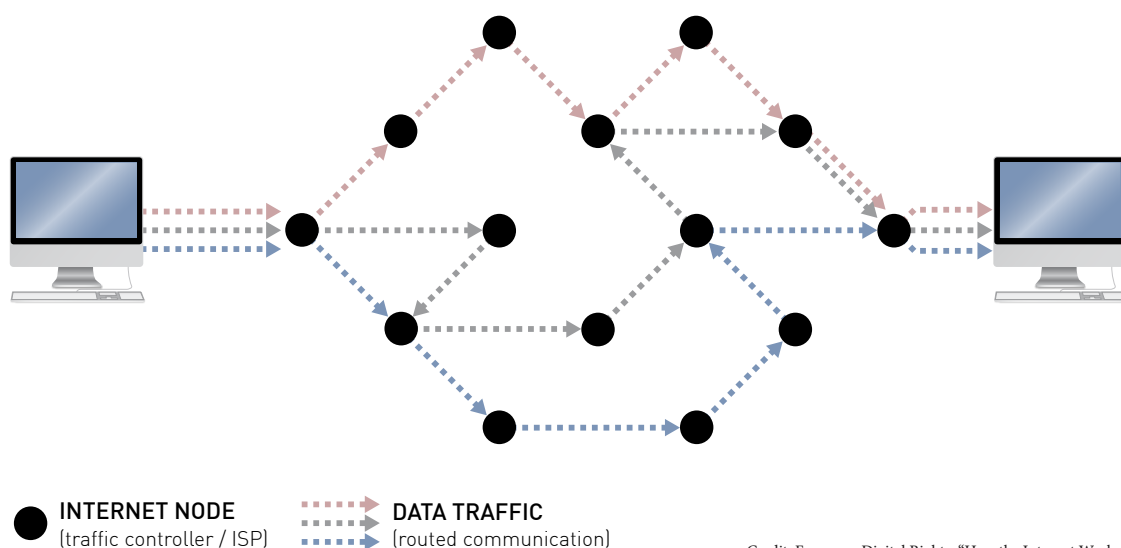
## THE INTERNET AND ONLINE INTERMEDIARIES

Policymaking online requires an understanding of the broad range of online intermediaries that provide services on the Internet, and how they relate to their end users. This, in turn, requires a basic understanding of the functioning of the Internet. This chapter seeks to address each of these questions. After first providing a basic introduction to the functioning of the Internet, this chapter attempts to provide a broad overview of the main types of online intermediaries, their functions, and how these functions relate to their potential for law enforcement cooperation. It then briefly discusses the nature of relations between online intermediaries and end users.

### WHAT IS THE INTERNET?

The Internet is a global network connecting billions of computers and other electronic devices by facilitating the transmission of digital data. Digital data is data which have been converted into a binary code consisting solely of ones and zeroes. Conversion of data into binary code makes digital networks vastly more efficient than traditional communications networks. Traditional communications networks, such as the telephone system, require a direct connection between the sender and receiver of a communication. This direct connection typically uses all or most of the available communications frequencies because data are sent via an electrical circuit. By contrast, when transmitting digital data, multiple different signals can be sent and received simultaneously.

Figure 1. A network of computer networks



Credit: European Digital Rights, "How the Internet Works."

The Internet is a highly efficient way of moving digital data. The Internet works by breaking digital files or other data into "packets", sending each "packet" via the most efficient route currently available on a system of interconnected networks (figure 1), before reassembling the file or other data at the destination. For different devices on the Internet to find each other, each needs an address. This address is known as an Internet protocol (IP) address, which is a string of numbers in a specific format. These are managed globally by five "Regional Internet Registries" which allocate "blocks" of IP addresses to service providers in the region of the world for which they are responsible.

The Internet and the World Wide Web (more commonly simply known as "the Web") are often confused, but the two terms have separate meanings. The Web refers to a system for the exchange of data identified by Uniform Resource Locators (URLs), transferred using the Hypertext Transfer Protocol (HTTP), and accessed by users using a web browser. The Web is just one way of transferring information over the Internet, albeit one of the most significant ways. Email, for example, is another way of transferring information over the Internet. Emails send data over the Internet, but not over the Web.

Each device on the Internet has an IP address. Each website is hosted on a server, which in turn has an IP address where it can be found. The domain name system, which translates domain names (such as [unodc.org](https://unodc.org)) into IP addresses, allows Internet users to browse the Internet using names rather than numbers. The same functionality is used for other purposes, such as email.

Domain names are organized according to top-level domains (TLDs) that are indicated at the end of the domain name. TLDs can either be "generic" (gTLDs), such as .com, .org or .net, or country-specific (ccTLDs), such as .ca, the ccTLD of Canada. TLDs are managed by domain name registry operators, who work with companies known as domain name registrars that rent domain names to end users called registrants. Broadly speaking, domain name registry operators can therefore be considered wholesale providers of domain names whereas domain name registrars can be considered retail providers.

This basic overview of the functioning of the Internet informs this chapter's discussion of the functions of various online intermediaries. Throughout this paper the term "online" is used to denote activities which take place over the Internet.



### WHAT IS THE DARKNET AND DARK WEB?

The darknet refers to encrypted networks (darknets) superimposed (or overlaid) on the Internet that can only be accessed using specific protocols.<sup>a</sup> The darknet is thus distinguished from the Internet according to the accessibility of the content found thereon.<sup>b</sup> The most well-known darknet is Tor.<sup>c</sup> Other darknets include the Invisible Internet Project (I2P) and Freenet.

The dark web refers to one way of transferring information over the darknet. Hence, the dark web is to the darknet what the World Wide Web is to the Internet. The dark web is distinguishable from the deep web and the surface web. The surface web refers to that part of the Web which is indexed by traditional web search engines and for this reason easily accessible to the general public. The deep web refers to the part of the Web which is not indexed by traditional web search engines. This includes intranet sites, academic databases, medical records, online banking, forums and social media pages with restricted access and content protected by paywalls, such as video streaming services. The dark web refers to web pages that are not only not indexed by traditional web search engines but which also can only be accessed using specific protocols, such as Tor.

Tor (whose name is derived from the project's original name "The Onion Router") relies on a technique for anonymous communication called "onion routing", which was originally designed by the United States Naval Research Laboratory in the mid-1990s.<sup>d</sup> Onion routing allows for private communications through the use of multiple layers of encrypted connections. A user connects to an "entry node", which establishes an encrypted connection to a second node. That second node establishes an encrypted connection to a third node, which in turn connects to the online resource to which the user is connecting. This system provides the user with anonymity: the first node knows who the user is (or at least, their IP address) but does not know where the communication is going. The third node knows where the communication is going but does not know who the user is. The second node knows neither who the user is or where the communication is going.

<sup>a</sup> Laurent Gayard, *Darknet: Geopolitics and Uses*, vol. 2 (London, ISTE; Hoboken, New Jersey, John Wiley and Sons, 2018), pp. 11 and 158.

<sup>b</sup> Ibid., p. 9.

<sup>c</sup> For more information, see <https://torproject.org>.

<sup>d</sup> For more information, see Espacenet, US6266704B1, "Onion routing network for securely moving data through communication networks", available at <https://worldwide.espacenet.com/>

### WHAT IS AN ONLINE INTERMEDIARY?

Access to the Internet and the variety of online services provided by individuals and organizations is facilitated by a diverse network of service providers referred to in this publication as "online intermediaries".<sup>68</sup> Online intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.<sup>69</sup>

Online intermediaries may exercise a range of different functions. Their services may be directly used by end users of the Internet or instead by other intermediaries. Online intermediaries may provide services on the physical, network and application layers of the Internet.<sup>70</sup>

<sup>68</sup> Such intermediaries are sometimes referred to as "Internet intermediaries", "online service providers" or "Internet service providers", among other terms. For further discussion of terminology, see Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford, Oxford University Press, 2016), pp. 26–36; Graeme B. Dinwoodie, "A comparative analysis of the secondary liability of online service providers", in *Secondary Liability of Internet Service Providers*, Graeme B. Dinwoodie, ed. (Cham, Switzerland, Springer International Publishing, 2017), pp. 1, 4–8; Graeme Dinwoodie, "Who are Internet intermediaries?", in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), p. 37.

<sup>69</sup> Organisation for Economic Co-operation and Development (OECD), "The economic and social role of Internet intermediaries" (April 2010), p. 9.

<sup>70</sup> For an explanation of this taxonomy of service providers, see Riordan, *The Liability of Internet Intermediaries*, pp. 36–46.

The vast majority of online intermediaries and their users have no intention of committing or facilitating crime. However, just as the services of online intermediaries are used for legitimate purposes, they may also be used by criminals to commit serious crimes online, such as the trafficking of wildlife, falsified medical products and cultural property. The purpose of this section is to provide a broad overview of the main types of online intermediaries, their functions, and how these functions relate to their potential for law enforcement cooperation. The capacity for online intermediaries to take effective and proportionate action against crime online varies considerably according to their functions. In general, the more direct the business relationship is between the online intermediary and the person using its services for criminal purposes, the more likely that the online intermediary will be able to take effective action, in relative terms.

An understanding of the respective functions of various online intermediaries is essential to developing policies to address serious crimes committed online, such as wildlife crime, falsified medical products-related crime and trafficking in cultural property. Measures which fail to take into account the differing functions of various online intermediaries are likely to be disproportionate and ineffective in achieving their intended outcomes, while having major negative consequences for individuals and organizations using the Internet, both in the jurisdiction in which the measures are imposed and elsewhere.

This section provides an overview of key online intermediaries which may potentially be relevant to online trafficking in wildlife, falsified medical products and in cultural property. These include Internet access providers, hosting service providers, social media service providers, cloud storage and cloud software providers, payment service providers, cryptocurrency providers, search engine providers, domain name registrars and instant messaging service providers.

Where this section identifies actions that can theoretically be taken by an online intermediary to address serious crimes committed online, this should not be understood as implying that such actions would necessarily be effective, proportionate or authorized by law. Rather, such references are intended to indicate the technical capacities of various online intermediaries.

## Internet access providers

Internet access providers (also known as Internet service providers (ISPs))<sup>71</sup> are service providers that permit individuals and organizations to access the Internet. This access can be provided through either a fixed connection (such as a wired broadband connection) or a mobile connection. Internet access providers typically keep logs of, at a minimum, the IP addresses allocated to their subscribers at particular times. Due to the peculiarities of mobile networks, mobile Internet access providers generally process more personal data of their subscribers than fixed Internet access providers, such as location data.

The information held by Internet access providers about their subscribers may be useful to law enforcement authorities in investigating wildlife crime, falsified medical products-related crime or trafficking in cultural property online. Access providers can usually identify which of their subscribers was connected to the Internet using a particular IP address at a particular moment, although this data is generally not stored indefinitely as this is not necessary for the provision of the service. Identifying the subscriber that was allocated a particular IP address does not, however, necessarily identify the individual user that was using the connection at that time. For example, some businesses and organizations such as cafés, libraries and city councils make Internet connections available to the public through publicly accessible Wi-Fi connections. In such cases, the Internet access provider will not have information about who is accessing the Internet through that connection.

Internet access providers can also assist law enforcement authorities investigating wildlife crime, falsified medical products-related crime or trafficking in cultural property online by taking steps to restrict or “block”

<sup>71</sup> The term “Internet service provider” is arguably more prevalent than “Internet access provider” to refer to this type of intermediary. Nevertheless, this paper avoids using the term “Internet service provider” because this term is sometimes erroneously understood to mean any service provider that provides a service over the Internet (in other words, any online intermediary), rather than one specific type of service provider.

access to particular websites. In practice, the effectiveness of such actions is limited because Internet access providers can only restrict the access of their subscribers and because most methods used for blocking access to particular websites are generally easy to circumvent, even for users with little technological know-how.

## Hosting providers

The term “hosting providers” traditionally referred to intermediaries that store (that is, “host”) websites on behalf of customers and make these websites accessible via the Internet. As various new types of online intermediaries emerged, use of this term has expanded to include intermediaries providing a broader range of services. Today, a hosting provider can be understood to be an intermediary whose services consist of, among other activities, the storage of any digital data provided by users,<sup>72</sup> and also includes blogging platforms, platforms for sharing media such as music or videos, cloud storage and cloud software providers, social media platforms, discussion forums and online marketplaces, among many others. The degree of interaction that the intermediary has with the content provided by users varies considerably between different types of hosting providers.

Hosting service providers can assist law enforcement and judicial authorities by providing access to data hosted on their servers, removing data from their servers, and sharing information about their users.

## Social media providers

Social media providers are hosting providers that allow users to create and share content or to participate in social networking with other users. In practice, many social media companies, such as Facebook, Weibo and Odnoklassniki, are clusters of services and may operate as data collectors, advertising networks, instant messaging services, online marketplaces and news aggregators, among other services, all at the same time. The exact services offered by social media providers vary between providers. Accordingly, it is more useful for policymakers to look at the various services offered by social media providers when developing policy measures, rather than treating social media providers as a homogenous group.

As with other hosting service providers, social media providers can assist law enforcement and judicial authorities by providing access to data hosted on their servers, removing data from their servers, and sharing information about their users. Some social media providers, particularly larger social media providers, also have access to more powerful tools that could also assist law enforcement and judicial authorities, albeit with varying degrees of intrusiveness, collateral damage and potentially counter-productive effects.<sup>73</sup> These include tools that attempt to automatically identify suspicious content and block the upload of known or suspected illegal content.

## Cloud storage and cloud software providers

Cloud computing refers to on-demand network access to a shared pool of configurable computing resources (including, for example, networks, servers, storage, applications and services) “that can be rapidly provisioned and released with minimal management effort or service provider interaction.”<sup>74</sup> Cloud computing can be used to carry out tasks that were previously performed locally on the user’s computer. Among

<sup>72</sup> This operating definition is based upon the definition used in European Commission, *Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape* (Luxembourg, Publications Office of the European Union, 2018), p. 10.

<sup>73</sup> In 2018, Facebook Chief Executive Officer Mark Zuckerberg noted that its content review teams make incorrect decisions in more than 10 per cent of cases, which amounts to approximately 300,000 incorrect decisions per day. See Mark Zuckerberg, “A blueprint for content governance and enforcement”, Facebook, 15 November 2018; Paul M. Barrett, “Who moderates the social media giants? a call to end outsourcing” (New York, NYU Stern Center for Business and Human Rights, 2020), p. 5.

<sup>74</sup> Peter Mell and Timothy Grance, “The NIST definition of cloud computing: recommendations of the National Institute of Standards and Technology”, Special publication 800-145 (Gaithersburg, Maryland, United States Department of Commerce, National Institute of Standards and Technology, 2011), p. 2.

providers of cloud services are cloud storage providers (such as Google Drive, Microsoft OneDrive and Baidu Cloud) which allow people to store files on the provider's servers as a complement or alternative to storing files on their own computer. Cloud service providers may also offer "software as a service", which refers to software applications that run on the provider's own infrastructure (cloud infrastructure) rather than that of the end user.

Cloud providers can block or remove accounts and remove access to particular services. Cloud providers also sometimes filter material that is being uploaded to their services to check for known illegal material. This works efficiently if appropriate actions are taken by all relevant stakeholders when an attempt to upload such material is identified and if the content in question is illegal regardless of its context (such as child sexual abuse material, for example). Transparency and independent testing are also needed to ensure accountability in such circumstances.

## Domain name registrars

Domain name registrars work with domain name registry operators to register domain names to be rented by individuals and organizations. Domain name registrars can, in certain circumstances, revoke domain names as a means of fighting illegal activity. Revocation of a domain name is, however, a relatively superficial measure as it does not remove the illegal content. Revoking a domain name is akin to removing a business phone number from the phone book. The business and its infrastructure would still be intact; it would simply be a little more difficult to find, at least until the business obtained a new phone number.

## Domain name registry operators

A domain name registry operator is an organization that manages top-level domain names (TLDs). When a registrant makes a request to rent a domain name from a domain name registrar, that registrar will request the registry operator to set up the particular domain name. The registrant relies on the registry operator to set up their domain name correctly but has no interactions with the registry operator.

Domain name registry operators can, like domain name registrars, revoke domain names in appropriate circumstances as a means of addressing illegal activity online. Law enforcement agencies may sometimes choose to engage with domain name registry operators as a means of bypassing or overriding uncooperative domain name registrars.<sup>75</sup> However, as noted above, revocation of a domain name is a relatively superficial measure as it does not remove the illegal content.

## Search engine providers

Search engines, such as Baidu, Bing, DuckDuckGo, Google or Yandex, are online services that are used by end users to search the Web. Search engine operators cannot prevent illegal content from being accessed but can take steps to prevent users from finding, or make it more difficult for users to find, particular illegal content through their service. In relation to illegal content on the Web, search engine providers can remove sites from their results,<sup>76</sup> not accept certain search terms, prevent certain search terms from displaying certain results<sup>77</sup> or demote certain search results. They can take these actions in relation to all searches or only searches made by users accessing the Internet from particular jurisdictions. Little research has, however, been undertaken as to the effectiveness of such actions.

<sup>75</sup> See, in relation to intellectual property rightsholders, Annemarie Bridy, "Addressing infringement: developments in content regulation in the US and the DNS", in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 631 and 637.

<sup>76</sup> As was the case in *Equustek Solutions Inc v. Google Inc*, 2015 BCCA 265.

<sup>77</sup> As was the case in *Google Spain SA v. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (commonly known as the "right to be forgotten" case), available at <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>.

## Instant messaging service providers

Instant messaging services allow users to send digital messages instantaneously using computers or mobile devices. Instant messaging services have expanded from offering the possibility to send text messages to also include voice and video calling functionality. Many providers of instant messaging services also offer end-to-end encryption of messages and calls. Instant messaging services can be stand-alone services or be linked to or embedded in other services such as social media platforms. Signal is an example of a stand-alone instant messaging service and Facebook Messenger is an example of a service embedded in a broader social media platform.

The data that providers of instant messaging services have about the messages sent over their services depend on whether the messages are encrypted. Where messages are encrypted from sender to the recipient(s), the providers themselves will not have access to the content of the messages, but rather only message metadata, such as the date and time the message was sent and the sender and recipient(s) of the message. Accordingly, whether messages and calls are encrypted is a significant factor in determining the extent to which instant messaging providers can provide assistance to law enforcement and judicial authorities. Providers of instant messaging services linked to or embedded in a broader service such as a social media service may also have broader data on users than providers of stand-alone instant messaging services. While such measures are by their very nature not sufficient to prevent access to illegal content, they can contribute to limiting its dissemination.

## Payment service providers

Payment service providers include online-specific payment services such as Alipay, PayPal, Paytm and Qiwi, and online banking and payment services provided by traditional banks. Each of these services allows users to send and receive payments online, including for online commerce. Payment service providers are often well placed to identify unusual activity and infringements and trace payments, often supported by advanced due diligence and “know your customer” procedures.

## Cryptocurrency-related service providers

Cryptocurrency providers refer to a group of different providers that grant access to cryptocurrency exchange, banking (“wallet”) and payment services. Cryptocurrencies are virtual currencies generally based on the “blockchain” or other distributed ledger technologies. Cryptocurrencies are often decentralized, allowing transactions to take place without being regulated or controlled by any centralized authority. Cryptocurrencies are sent and received using public and private keys – strings of letters and numbers that function in pairs. Public keys are used to receive payments and private keys, which are analogous to passwords, are used to make payments. Cryptocurrencies may be sent to “addresses”, which are generated from public keys using a cryptographic hash function. Cryptocurrency “wallets” are software programs that store private and public keys on behalf of a user.

Cryptocurrencies offer a degree of privacy protection to their users which may be attractive to criminals. At the same time, cryptocurrencies may also pose opportunities for law enforcement to trace illicit transactions.<sup>78</sup> Complexities with making payments using cryptocurrencies may also make them unattractive for sales of illicit products to the general public, such as for the sale of falsified medical products by illegal online pharmacies. Law enforcement operations targeting the sale of falsified medical products online have found that while cryptocurrency payment options are available, they are not widespread. For example, less than 2 per cent of the illicit online pharmacies targeted by INTERPOL’s Operation Pangea XI in 2018 offered cryptocurrency payment options.<sup>79</sup>

<sup>78</sup> See, Giannis Tziakouris, “Cryptocurrencies: a forensic challenge or opportunity for law enforcement? An INTERPOL perspective”, *IEEE Security & Privacy*, vol. 16, No. 4 (August 2018), p. 92.

<sup>79</sup> Data supplied by INTERPOL for the purposes of this issue paper.

## RELATIONS BETWEEN ONLINE INTERMEDIARIES AND THEIR USERS

This chapter has shown how individuals and organizations rely on the services of a variety of online intermediaries to use the Internet for personal and professional purposes. Some of these services are directly used by end users of the Internet, whereas other services are not directly used by end users of the Internet but are nevertheless necessary for the use of the Internet. Unlike offline activity, all activity online is dependent upon multiple intermediaries.

The use of the services of online intermediaries is governed not only by any applicable law but also contractual relations. Contracts for the use of services of online intermediaries are commonly known as “terms of service”.<sup>80</sup> Where an individual or organization directly uses the services of an online intermediary, such as an Internet access provider, a web host, a social media provider or an online payment provider, the use of that service will be governed by applicable terms of service. Individuals and organizations may also be affected by the terms of service of online intermediaries that they do not directly use. For example, a domain name registry operator may require that the domain name registrars it contracts with impose certain conditions upon domain name registrants.

In the vast majority of cases, terms of service for the use of the services of online intermediaries are contracts of adhesion, also known as standard form contracts. Contracts of adhesion refer to contracts that are drafted by one party (usually with greater bargaining power – in this case, the service provider), which are offered to a counter-party (usually with weaker bargaining power – in this case, the end user or another service provider) on a “take it or leave it” basis. The counter-party must either agree to the terms of service proposed by the intermediary or forego use of that intermediary’s service.

Terms of service are often long, complicated and vague. They are frequently drafted to afford the intermediary with a broad discretion for dealing with unwelcome behaviour on the intermediary’s service, as intermediaries have little incentive to restrict their own room for manoeuvre.

### EXAMPLE

The following term provides a real example of the broad discretion that terms of service often afford online intermediaries:

You acknowledge that [the intermediary] may or may not pre-screen Content, but that [the intermediary] and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse or remove any Content that is available via the [intermediary’s services]. Without limiting the foregoing, [the intermediary] and its designees shall have the right to remove any Content that violates the TOS or is otherwise objectionable.<sup>a</sup>

<sup>a</sup> Jamila Venturini and others, *Terms of Service and Human Rights: An Analysis of Online Platform Contracts*, 2nd ed. (Rio de Janeiro, Brazil, Editora Revan, 2016), p. 53.

<sup>80</sup> They may, however, be referred to by other names, such as “community guidelines”.



The significant extent to which individuals and organizations, as end users of the Internet, rely upon multiple online intermediaries to conduct themselves online means that the rules which govern access to and the use of online services have important implications for the exercise of human rights such as freedom of expression and the right to peaceful assembly.<sup>81</sup> Human rights dimensions to policy responses to wildlife crime, falsified medical products-related crime and trafficking in cultural property online are further discussed in chapter 5.

## CONCLUSION

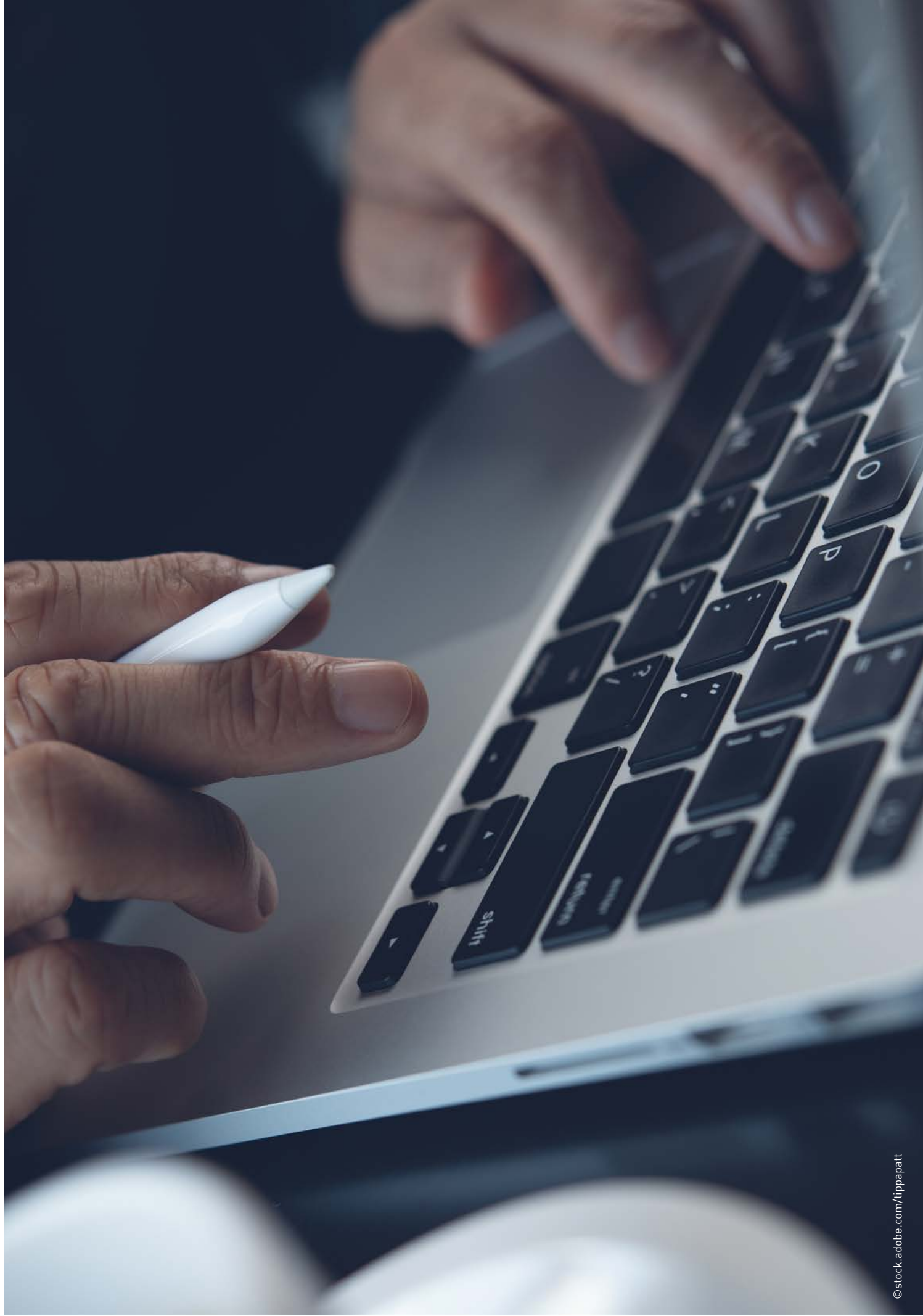
This chapter has sought to provide the reader with a foundational understanding of the operation of the Internet and the functions of online intermediaries as a base from which policy approaches to serious crimes committed through online intermediaries can be considered. It has done so through first explaining what the Internet is, providing an overview of the online intermediaries most relevant to the crimes covered by this paper, and finally discussing the nature of relations between online intermediaries and their users.

This chapter has shown that any individual or organization relies on a complex chain of online intermediaries to access and use the Internet. There are several key implications of this for policymakers. First, the intermediaries which an Internet user (including a criminal) relies upon to conduct themselves on the Internet are multiple and may be located in various jurisdictions. This poses challenges to effectively preventing and combating wildlife crime, falsified medical products-related crime and trafficking in cultural property online. Issues relating to jurisdiction are further discussed in chapter 4.

Secondly, the use of online services by individuals and organizations is governed not only by multiple applicable laws, both in the jurisdiction of residence of the end user and the jurisdiction in which the intermediary is based, but also by the contractual terms of service of multiple online intermediaries, including intermediaries with which an end user has no direct relationship. These laws and terms of service restrict what users can do online and hence can potentially affect the exercise of their human rights. The complex framework of laws and contractual rules governing access to and use of online services, and their effects on the enjoyment of human rights, must be considered in order to develop effective and proportionate approaches to preventing and combating serious crimes committed online. Relevant human rights issues are further discussed in chapter 5.

Thirdly, the various functions of online intermediaries and various relations of these intermediaries to their end users are reflected in differing capacities to take action to prevent and combat serious crimes committed by their users. Not all online intermediaries are equally capable of taking effective action against criminals operating online. For example, a domain name registrar or registry operator may be less likely to be able to take effective action than a hosting provider or a payment service provider. A domain name registrar or registry operator can withdraw a domain name used by an illicit online pharmacy, but such action has no effect on the underlying website. Conversely, a hosting provider, which can take an entire website offline, or a payment service provider, which may be able to cut off the website owner's illicit revenue, may be able to take more effective action against an illicit online pharmacy. Furthermore, not all online intermediaries have equal capacity for *proportionate* action. An Internet access provider could attempt to block its subscribers' access to a server on which the website of an illicit online pharmacy is hosted, but this could possibly block access to the hundreds or thousands of legitimate websites hosted on the same server. In general, the closer the interaction between an online intermediary and a criminal and the greater the degree of control they can exercise over the activities of the criminal, the more likely it is that the online intermediary will be able to take effective and proportionate action.

<sup>81</sup> Thus, the Human Rights Committee has noted that "increased private ownership and other forms of control of public accessible spaces and communication platforms" must inform a contemporary understanding of the right to peaceful assembly. See Human Rights Committee, general comment No. 37 (2020) on the right of peaceful assembly, para. 10.



---

# Chapter 3.

## STAKEHOLDERS AND THEIR INTERESTS

In the previous chapter, this issue paper considered, among other things, the broad range of online intermediaries and their relations to their users. This chapter now zooms out from individual types of intermediaries to consider the broad groups of stakeholders whose interests States must protect and promote when developing policies to prevent and combat wildlife crime, falsified medical products-related crime and trafficking in cultural property online. These key stakeholders are the public, including both the individuals and businesses that use the Internet, and online intermediaries themselves.

### THE PUBLIC

Consideration of the interests of the public is important because it is the public that is ultimately affected by serious crime. It is the interests of the public that measures to prevent falsified medical products and trafficking in cultural property seek to protect and promote. Measures to prevent and combat wildlife crime also seek to protect and promote the interests of the public, along with environmental interests and the interests of wild flora and fauna.

The interests of the public – whether individuals or organizations – are multiple and at times pull in different directions. One interest cannot be privileged to the exclusion of all others. This section first considers the interests of individuals and then organizations.

### Individuals

At least two interests of individuals, as members of the public and users of the Internet, are relevant to wildlife crime, falsified medical products-related crime and trafficking in cultural property committed online. These are protection from crime and protection from unjustified interference with human rights.

As was further outlined in chapter 1, the crimes with which this paper is concerned are serious crimes with significant detrimental consequences. Falsified medical products endanger life and health, among other negative public health consequences. Wildlife crime damages the environment, ecosystems and biodiversity, which can have long-term consequences for the entire planet and humankind. Trafficking in cultural property attacks the common heritage of humankind and the culture and identity of peoples. The public's interest in protection from each of these destructive crimes has been repeatedly recognized by the international community.

The public's interest in protection from these crimes necessarily implies an interest that States do not undertake measures that are counterproductive to or ineffective in addressing these crimes.<sup>82</sup> Accordingly, the public has an interest in evidence-based policy and the diligent monitoring, evaluation and adaptation of measures taken to prevent and combat these crimes.

Individuals also have an important interest in the protection and promotion of their human rights. This requires that measures taken to address wildlife crime, falsified medical product-related crime and trafficking in cultural property online be proportionate, both when they are established and on an ongoing basis as the nature of both these crimes and information and communications technologies change over time. Human rights dimensions to policy responses to these crimes are further discussed in chapter 5.

## Businesses

Businesses, like individuals, also have multiple interests which are relevant to policymaking to address wildlife crime, falsified medical products-related crime or trafficking in cultural property committed online. These, too, may pull in different directions. Like individuals, businesses have an interest in protection from crime. Insofar as crimes covered by this paper impact upon licit markets, businesses also have a direct commercial interest in preventing and combating these crimes. Falsified medical products, for example, have negative economic impacts on legitimate manufacturers of medicines and medical devices.

Businesses also have an interest that policy measures to address these crimes online are predictable, transparent and proportionate to their legitimate aim. Chapter 2 demonstrated how every business operating online relies on a complex chain of online intermediaries, many of which are often based in a different jurisdiction. If the policy environment in any of these countries creates excessive legal risk or uncertainty for online intermediaries, this can have a significant impact on the availability of online services for legitimate businesses. Online intermediaries faced with excessive legal risk or uncertainty may choose to suspend services for legitimate users or ban entire areas of legitimate economic activity to avoid liability. Consequently, there is a strong business interest that measures establishing liability of online intermediaries be proportionate, predictable and effective as to their intended outcomes, both when introduced and on an ongoing basis. In this regard, the Committee of Ministers of the Council of Europe has stated that legislation applicable to online intermediaries should be accessible, foreseeable, "clear and sufficiently precise to enable intermediaries, users and affected parties to regulate their conduct".<sup>83</sup>

## ONLINE INTERMEDIARIES

In addition to their roles as members of the public and members of the broader business community, online intermediaries have particular interests which must be considered by policymakers in developing measures to prevent and combat wildlife crime, falsified medical products-related crime or trafficking in cultural property online. The interests of online intermediaries are not homogenous and may vary in accordance with a number of factors including their functions, business model, size, market share and geographical spread. For example, an online intermediary that offers a free service and which relies on advertising revenue will be impacted less by requirements to suspend services to individual users than a competitor that relies on a user subscription model for income. A larger intermediary will gain a competitive advantage over smaller intermediaries from any policy measures that create or increase barriers to entry or growth in the industry, such as obligations to implement expensive technologies. An intermediary operating in a single jurisdiction will not be impacted by contradictory legislation in a neighbouring jurisdiction whereas a competitor active in both jurisdictions may

<sup>82</sup> An example of how certain measures to prevent and combat wildlife crime, falsified medical products-related crime or trafficking in cultural property online may be counterproductive to their goals is discussed in this chapter in the section on the interests of online intermediaries.

<sup>83</sup> Council of Europe, Committee of Ministers, "Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities" (Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, appendix, para. 1.2.1).

be heavily impacted. The diverse interests of online intermediaries must be considered when developing measures to prevent and combat wildlife crime, falsified medical products-related crime or trafficking in cultural property online. This in turn underscores the need for a multi-stakeholder approach to policy development.

Despite the differing interests of various online intermediaries, some generalizations can be made. First, it must be noted that the vast majority of online intermediaries have no intention of committing or facilitating serious crime and would like to assist in preventing and combating such crime where this can be done in a manner that is compatible with the achievement of their commercial objectives. Only a very small number of online intermediaries provide their services with the specific intention of facilitating illegal activity. These rogue actors are not the focus of this issue paper. They “act under a different logic and incentive structure” to other online intermediaries and require a different policy response.<sup>84</sup>

Second, whether the commercial interests of an online intermediary support taking action to prevent its services being used for criminal activity depends on a variety of factors. Factors that support taking action to prevent a particular crime include the direct costs of such crimes to the intermediary and the extent to which the crime negatively affects user experience.<sup>85</sup> Email spam, for example, directly costs email providers money in terms of the storage and bandwidth used by the spam. Furthermore, spam emails may lead to a provider losing dissatisfied customers. Accordingly, email providers have strong commercial incentives to prevent email spam. Operators of online marketplaces also have strong commercial interests to prevent users from being defrauded as this may discourage users from returning to their site. Additionally, online intermediaries may have incentives to take action against criminal activity because of the reputational risk of being associated with such activity.<sup>86</sup>

In general, online intermediaries have comparatively weaker incentives to take action against the three types of crime covered by this paper. Firstly, the direct costs of wildlife crime, falsified medical products-related crime and trafficking in cultural property to online intermediaries are likely to be negligible. Additionally, the reputational risks of being associated with these illicit activities are comparatively weaker for online intermediaries. These crimes receive comparatively less media attention than others such as terrorism and the distribution of child sexual abuse material and, despite the significant harms they cause, are commonly considered to be less serious than such crimes. Furthermore, where buyers and sellers of illicit wildlife products and cultural goods are mutually satisfied with their transaction, online intermediaries may not suffer from unhappy users. In contrast, falsified medical products may cause harm to purchasers and hence online marketplaces which offer the possibility for trade in medical products have an incentive to prevent the sale of medical products which are falsified or substandard.

Weighing against incentives for an online intermediary to take action against the use of its services for illicit purposes are several countervailing factors.<sup>87</sup> Implementing measures to detect, prevent and respond to illegal activities may involve substantial costs for online intermediaries. Such costs will be particularly burdensome for smaller online intermediaries. Actions such as the removal of content or the suspension of users directly result in lost business for online intermediaries and hence online intermediaries have an interest in not taking such actions any more than is necessary. Additionally, the actions of online intermediaries in detecting, preventing and responding to the illicit use of their services may negatively affect the user experience of other users, or a segment thereof. This may create further costs for the intermediary.

Third, the balance of incentives for online intermediaries is also affected by the policy environment in which they operate. Policymakers should be careful to ensure that policy frameworks encourage effective cooperation from online intermediaries and to avoid providing online intermediaries with commercial disincentives to act in ways that assist the effective investigation and prosecution of serious crime online. Otherwise, policies seeking to prevent and combat wildlife crime, falsified medical products-related crime or trafficking

<sup>84</sup> European Commission, *Hosting Intermediary Services and Illegal Content Online*, pp. 24–25.

<sup>85</sup> Giancarlo Frosio and Martin Huvosec, “Accountability and responsibility of online intermediaries”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 613 and 625.

<sup>86</sup> European Commission, *Hosting Intermediary Services and Illegal Content Online*, p. 22.

<sup>87</sup> *Ibid.*, p. 23.



in cultural property online can have counterproductive effects. For example, where a law exposes an online intermediary to liability for failing to take adequate steps to prevent the sale of illicit products, online intermediaries will be incentivized to quickly take steps to remove content it considers to be potentially illegal. If the removal of such content is done without cooperation from law enforcement authorities, this may interfere with ongoing investigations. To address this issue, the laws of some countries require that online intermediaries preserve data and report particular forms of illegal activity to authorities in carefully circumscribed circumstances.<sup>88</sup>

The balance of incentives for online intermediaries is affected not only by present policy frameworks but also the spectre of future policy interventions. For example, some domain name registry operators have supported pre-emptive self-regulation as a means of warding off government intervention that might entail more onerous obligations.<sup>89</sup> In such cases, it should be borne in mind that the “problem” being addressed by the online intermediary is the threat of future regulation rather than the illicit conduct in question. Actions by online intermediaries in such circumstances are hence less likely to be effective than measures that seek to address the illicit conduct directly.

Fourth, for the attainment of their legitimate commercial objectives, online intermediaries need a clear legal framework in which they can operate, both within and across jurisdictions. This is also important for online intermediaries to effectively cooperate with law enforcement. Contradictory legal obligations between different jurisdictions can be a significant factor in dissuading intermediaries from assisting law enforcement more actively.

Finally, as private companies with their own interests and incentives, online intermediaries are institutionally ill-equipped for making difficult decisions involving the balancing of multiple competing public interests and human rights,<sup>90</sup> such as the type of decisions discussed in chapter 5 of this paper. Online intermediaries “will inherently try to lower the transaction costs” of adjudicating claims between competing interests and have commercial incentives to “functionally err on the side of overblocking”.<sup>91</sup> A case study which highlights this risk is set out below.

#### CASE STUDY. NOTICE AND TAKEDOWN IN RELATION TO HUMAN RIGHTS

A case study involving an online hub for people with diabetes with a focus on technologies for treating their condition provides an example of the challenges faced by online intermediaries in assessing competing claims of users and third parties, and the pitfalls of online intermediaries making such assessments. The administrator of this hub published technical instructions and code for extracting blood-sugar data from a glucose monitoring device sold by a third-party company. This code was published on the website of a prominent United States-based code repository.

The third-party company issued a takedown notice to the code repository under the United States Digital Millennium Copyright Act (DMCA), claiming that the code constituted an unauthorized derivative work of its software and that the extraction of blood-sugar data from its devices constituted circumvention of a copyright protection system, each in violation of United States copyright law.<sup>92</sup> The company requested that the code

<sup>88</sup> Examples of such requirements are further provided in chapter 4.

<sup>89</sup> Bridy, “Addressing infringement”.

<sup>90</sup> Giancarlo Frosio, “Mapping online intermediary liability”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 1 and 26.

<sup>91</sup> Ibid.



repository remove and disable access to the code and take steps to prevent alleged further infringement and violations. The takedown notice further noted that failure to do so could lead to the code repository being liable for compensatory damages, disgorgement of profits and costs of legal representation.

The code repository, which was ill-placed to assess the merits of the legal basis for the takedown notice, was faced with the choice between risking liability for failure to comply with the notice and removing the code in question. It chose to remove the code.<sup>b</sup>

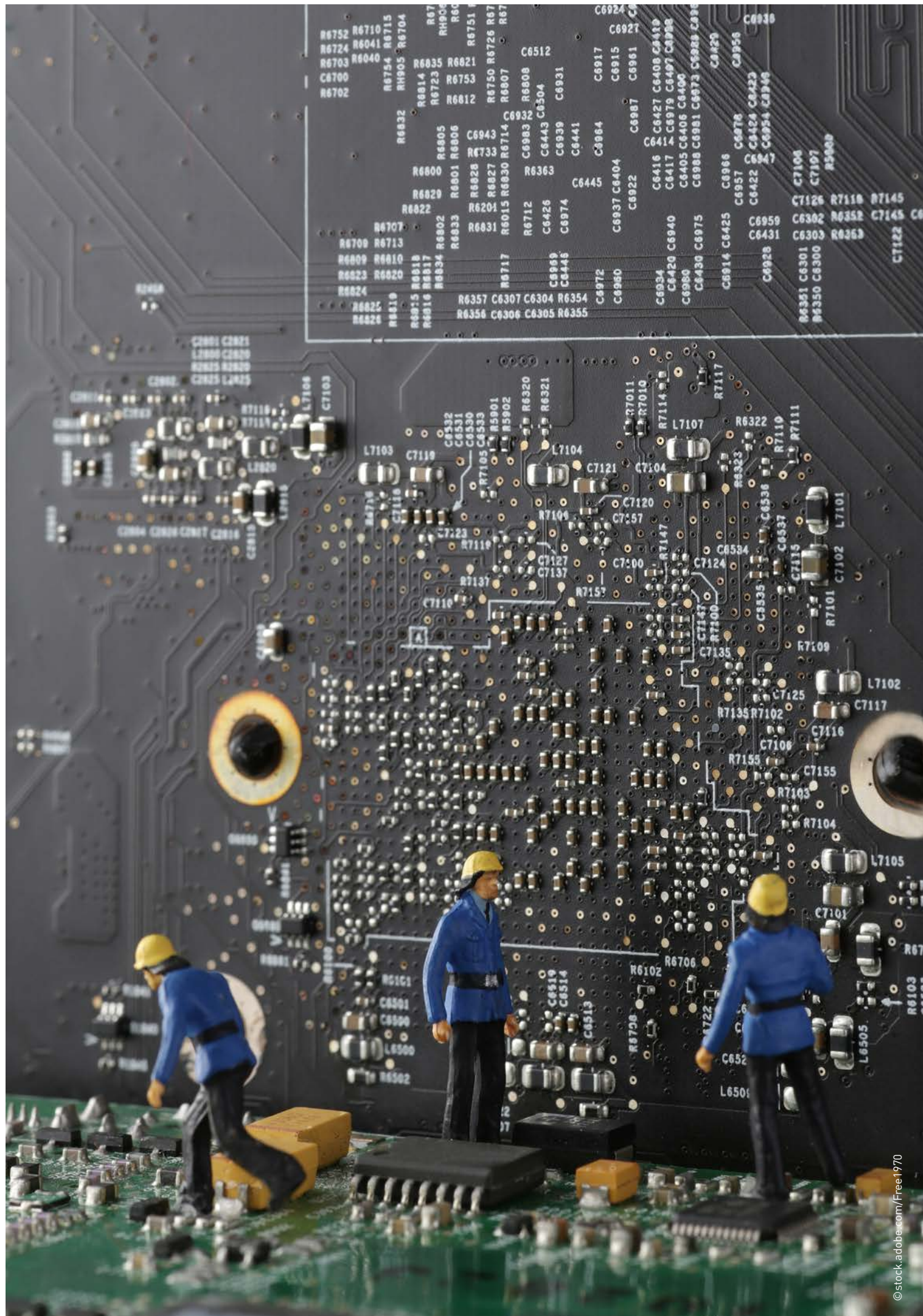
<sup>a</sup> GitHub, 2019-11-08-abbott.md, “hubot Process DMCA request”, 8 November 2019, available at <https://github.com/github/dmca/blob/master/2019/11/2019-11-08-abbott.md>.

<sup>b</sup> See further Cory Doctorow, “Abbott labs kills free tool that lets you own the blood-sugar data from your glucose monitor, saying it violates copyright law”, Boing Boing, 12 December 2019.

## CONCLUSION

The online ecosystem is a web of overlapping interests and needs. The brief overview of the interests of key stakeholders provided in this chapter has shown that these interests are multiple and can pull in different directions – both between and within groups of stakeholders. Individuals, as members of the public, have an interest in protection from the destructive effects of wildlife crime, falsified medical products-related crime and trafficking in cultural property. They also have an interest in the protection and fulfilment of their human rights, which as discussed in detail in chapter 5, both require that States take action to prevent and combat the crimes covered by this issue paper and restrict the actions that States can take in pursuit of these ends. Businesses, like individuals, also have an interest in protection from the destructive effects of these crimes, but need policy measures, particularly legislation, addressing these crimes online to be clear, proportionate and predictable. Likewise, while the interests of online intermediaries vary depending on their functions, business model, size, market share and geographical spread, they too have an interest that policy measures addressing these crimes be clear, proportionate, predictable and competitively neutral.

Approaches to preventing and combating wildlife crime, falsified medical products-related crime and trafficking in cultural property online must take into account this complex web of interests and effectively balance the interests of all key stakeholders. Policymakers should be aware that certain policy measures may have the effect that online intermediaries take actions which are counterproductive to the investigation of these crimes or which interfere with the rights of legitimate individuals or organizational users and ensure that policy measures provide appropriate incentives for online intermediaries to take actions which help, rather than hinder, law enforcement investigations and which fully respect the rights of their users.



---

# *Chapter 4.*

## POLICY MEASURES FOR ADDRESSING SELECTED TYPES OF CRIME COMMITTED THROUGH ONLINE INTERMEDIARIES

Having now considered the problems that this issue paper seeks to address, the nature of the Internet, the variety of online intermediaries and the interests of key stakeholders in chapters 1, 2 and 3 respectively, this paper now turns to consider several broad categories of policy measures for addressing wildlife crime, falsified medical products-related crime and trafficking in cultural property online and the key considerations and issues relating to each type.

There are several different ways of classifying policy measures for addressing serious crime committed online. The first way of classifying policy measures is according to whether these measures are “horizontal” or “vertical”. Horizontal measures refer to measures that apply to all online intermediaries, all types of illegal activity committed online or both. In contrast to horizontal measures, vertical measures are those that apply to only some online intermediaries, only some types of illegal activity or both. Measures that only concern Internet access providers, or measures that only concern online trafficking in cultural property could both be considered vertical measures, for example. Both the terms horizontal and vertical measures hence carry a degree of ambiguity as to whether they are referring to intermediaries, types of illegal activity, or both. Where each of these terms is used in this paper, the relevant sense in which the term is used is specified.

A second way of classifying policy measures is according to whether they are based on the imposition of liability for online intermediaries for taking or failing to take certain actions (referred to in this paper as liability-based measures) or non-coercive cooperation with online intermediaries (referred to in this paper as cooperation-based measures). This is the primary classification adopted by this paper to discuss various



policy approaches to addressing wildlife crime, falsified medical products-related crime and trafficking in cultural property online. It should be noted, however, that these measures are not mutually exclusive. The overall policy approach taken by a State to address wildlife crime, falsified medical products-related crime and trafficking in cultural property online may involve both cooperation-based and liability-based measures. Indeed, some specific policy measures do involve both, such as conditions for access to statutory safe harbours that require an online intermediary to have adopted and implemented the code of conduct of an industry representative body, as well liability for failure to cooperate with authorities in specified circumstances.

This chapter first examines cooperation-based approaches before examining liability-based approaches and several issues common to both types of approaches. Various legislative examples are included in this chapter showing how States have implemented these approaches in practice.

#### Disclaimer

The legislative examples discussed in this chapter are included for the purpose of illustrating the variety of approaches taken by States. The inclusion of a legislative example should not be considered to be an endorsement of a provision, an approach, or the legislative scheme in which it is found.

## COOPERATION-BASED MEASURES

Cooperation-based measures involve policymakers seeking to have industry cooperate with law enforcement authorities to prevent and combat illicit activity online. In the vast majority of cases, the online intermediaries whose services are used to commit crime do not want criminal activity happening on or over their networks.

Cooperation-based measures may be based on self-regulatory or co-regulatory approaches. Self-regulatory approaches are approaches whereby private actors take measures, either on their own or as part of an industry sector, to regulate their own activities in order to achieve specific goals, such as minimum quality levels or broader public policy goals such as crime prevention. Self-regulation has been used in a wide variety of industries, with varying degrees of success.<sup>92</sup> Self-regulatory schemes can take the form of codes of practice, voluntary standards and accreditation arrangements. Co-regulatory approaches are similar to self-regulatory approaches, but involve the State directly engaging with industry to perform regulatory functions. In practice, concepts of self-regulation and co-regulation exist on a continuum of policy approaches and involve a considerable degree of overlap. Some scholars have attempted to develop a typology of types of self-regulation and co-regulation along this continuum.<sup>93</sup>

<sup>92</sup> Lisa L. Sharma et al, “The food industry and self-regulation: standards to promote success and to avoid public health failures”, *American Journal of Public Health*, vol. 100, No. 2 (February 2010).

<sup>93</sup> See, for example, Christopher T. Marsden, “Internet co-regulation and constitutionalism: towards European judicial review”, *International Review of Law, Computers & Technology*, vol. 26, Nos. 2 and 3 (July 2012), p. 211.

Through their policymaking, States may encourage online intermediaries to adopt self-regulatory measures or to work with the State to develop co-regulatory measures.<sup>94</sup> Article 16 of the European Union E-Commerce Directive, set out below, provides that Member States and the European Commission shall encourage the development of codes of conduct designed to contribute to the proper implementation of the Directive. Likewise, laws governing online intermediaries in Africa and the Caribbean also encourage the development of codes of conduct for online intermediaries with varying degrees of government involvement. Excerpts of the relevant legislation of the Bahamas and Ghana are also set out below.

#### EXAMPLE: EUROPEAN UNION – E-COMMERCE DIRECTIVE

##### Article 16

##### Codes of conduct

1. Member States and the Commission shall encourage:
  - (a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;
  - (b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;
  - (c) the accessibility of these codes of conduct in the Community languages by electronic means;
  - (d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;
  - (e) the drawing up of codes of conduct regarding the protection of minors and human dignity.
2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme.*

<sup>94</sup> See, for example, the European Union General Data Protection Regulation (GDPR) or E-Commerce Directive.



**EXAMPLE: BAHAMAS – ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT****Codes of conduct and standards for intermediaries and e-commerce service providers**

21. (1) If a code of conduct is approved or a standard is appointed by the Minister under this section to apply to intermediaries or e-commerce service providers, those intermediaries or e-commerce service providers shall comply with such code of conduct or standard.

(2) An intermediary or e-commerce service provider who fails to comply with an approved code of conduct or appointed standard, shall in the first instance be given a written warning by the Minister and the Minister may direct that person to cease and desist or otherwise to correct his practices, and, if that person fails to do so within such period as may be specified in the direction, he commits an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars and if the offence is a continuing one to a further fine of five hundred dollars for each day the offence continues.

(3) If the Minister is satisfied that a body or organization represents intermediaries or e-commerce service providers, the Minister may, by notice given to the body or organization, request the body or organization to —

- (a) develop a code of conduct that applies to intermediaries or e-commerce service providers and that deals with one or more specified matters relating to the provision of services by those intermediaries or e-commerce service providers; and
- (b) provide a copy of that code of conduct to the Minister within such time as may be specified in the request.

(4) If the Minister is satisfied with the code of conduct provided under subsection (3), the Minister shall approve the code of conduct by notice published in the Gazette and thereupon the code of conduct will apply to intermediaries or e-commerce service providers as the case may be, as may be specified in the notice.

(5) If the Minister is satisfied that —

- (a) no body or organization represents intermediaries or e-commerce service providers; or
- (b) a body or organization to which notice is given under subsection (3) has not complied with the request of the Minister under that subsection, the Minister may, by notice published in the Gazette, appoint a standard that applies to intermediaries or e-commerce service providers.

(6) If the Minister has approved a code of conduct or appointed a standard that applies to intermediaries or e-commerce service providers and —

- (a) the Minister receives notice from a body or organization representing intermediaries or e-commerce service providers of proposals to amend the code of conduct or standard; or
- (b) the Minister no longer considers that the code of conduct or standard is appropriate, the Minister may, by notice published in the Gazette, revoke or amend any existing code of conduct or standard.

(7) References in this section to intermediaries or e-commerce service providers include reference to a particular class of intermediary or e-commerce service provider.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

**EXAMPLE: GHANA – ELECTRONIC TRANSACTIONS ACT, 2008****Establishment of Industry Forum**

88. (1) There is hereby established an Industry Forum which shall be a platform to bring the industry together from time to time to discuss matters of common interest that relate to the industry.

(2) The Agency may designate an industry body to be the Forum by notifying that body in writing if the Agency is satisfied that

- (a) the membership of the body is open to the relevant parties and is fully representative of the industry,
- (b) the body is capable of performing as required under the relevant provisions of this Act, and
- (c) the body has the administrative capacity to service the Forum.

(3) The body shall agree in writing to be the Forum, before being designated by the Agency.

(4) Despite the designation, each licensed entity under the Act is deemed to be a member of the Forum.

(5) The Agency may decide that an existing industry body that was previously designated under subsection (2) to be an Industry Forum is no longer an Industry Forum if satisfied that the body does not meet the requirements of this section any longer.

(6) A designation or withdrawal of designation under this section takes effect from the date specified by the Agency.

(7) Until the Agency designates a body, the Agency has the obligation to facilitate the meeting of the industry to perform the functions of the Forum.

(8) The Ministry and the Agency shall participate in the Forum as observers.

**Industry code**

89. (1) The Forum may prepare a voluntary industry code to deal with a matter provided for in this Act

- (a) on its own initiative, or
- (b) at the request of the Agency.

(2) The code shall not be effective until it is registered by the Agency.

(3) The Agency shall register a voluntary industry code if it is consistent with

- (a) the objects of this Act,
- (b) regulations, standards or guidelines made under this Act, and
- (c) provisions of this Act which are relevant to the particular matter or activity.

(4) The Agency may refuse to register the code, if the Agency is not satisfied that there has been sufficient opportunity for public consultation in the development of the code by the Forum.

(5) The Agency shall notify the Forum in writing and provide the reasons for the refusal to register the code within thirty days after the refusal.

(6) Where the Agency does not register or refuses to register a voluntary industry code within a period of thirty days after the date that the voluntary industry code was submitted for registration, the Agency is deemed to have refused the registration of the voluntary industry code unless the Industry Forum receives a written notice of registration of the voluntary industry code after that period.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

There is an extensive body of literature examining the potential advantages and disadvantages to self-regulatory and co-regulatory approaches in various industries. The Organisation for Economic Co-operation and Development has identified several key factors upon which the success of any self-regulatory or co-regulatory scheme depends. These include the strength of the commitments made by participants, the extent to which the scheme covers the industry in question, the extent to which participants adhere to their commitments and the consequences of not doing so.<sup>95</sup>

In the context of preventing and combating crime online, there are further factors that influence the success or failure of self-regulatory and co-regulatory approaches. First, the impact of these schemes depends upon the extent to which intermediaries in the relevant industry exercise relevant control to prevent and combat the conduct in question. As noted in chapter 2, different types of online intermediaries have varying capacities to take action to prevent and combat serious crimes committed by their users. Not all online intermediaries are equally capable of taking effective and proportionate action against criminals operating online.

Second, the extent to which the interests of online intermediaries align with public policy goals is a significant factor in determining the success or failure of self-regulatory and co-regulatory approaches. Where the interests of online intermediaries (including, where relevant, the interests of their users) align with policy goals, self-regulatory or co-regulatory approaches are more likely to be successful. The issue of preventing and combating email spam provides an example of this. As noted in chapter 3, email providers are able to effectively self-regulate to prevent and combat email spam with minimal regulatory incentives to do so because stopping email spam is in their own interests. Email spam costs providers money in terms of storage space, bandwidth and customer dissatisfaction. Additionally, providers have incentives to not overly aggressively filter emails because lost, legitimate emails would cost them customers. Furthermore, email providers exercise the technical control necessary to take appropriate actions to fight email spam. When the interests of online intermediaries and the policy goals of States are aligned such that intermediaries share incentives to implement effective and proportionate measures, it is possible for self-regulatory and co-regulatory approaches to be successful with comparatively less legislative intervention.

Conversely, where online intermediaries do not have commercial incentives to address crimes taking place over their services, the chances of self-regulatory and co-regulatory approaches being successful are lower, particularly for self-regulatory approaches. This poses challenges to self-regulatory and co-regulatory schemes that seek to promote public goods, such as preventing and combating wildlife crime, falsified medical products-related crime and trafficking in cultural property. The extent to which online intermediaries also have an interest in preventing and combating these crimes in an effective and proportionate manner is likely to have a strong influence on the success of any self-regulatory or co-regulatory approach in this area. In this context, it is important to again note that there is a public interest in preventing and combating these crimes in a manner compatible with human rights such as freedom of expression, the right of peaceful assembly and the right to privacy. States should ensure that incentives given to online intermediaries to prevent and combat these crimes online do not lead to intermediaries taking measures that interfere with the exercise of these rights or the work of law enforcement. This may mean that co-regulatory approaches or approaches involving legally-mandated regulatory measures are more appropriate than self-regulatory approaches.

There are further factors which are critical to the success or failure of self-regulatory and co-regulatory approaches, such as the extent to which measures are appropriately adapted to different types of crime and the extent to which their success is effectively monitored, evaluated and adapted where appropriate. These factors are discussed later in this chapter under the section on issues common to cooperation- and liability-based approaches.

<sup>95</sup> OECD, *Industry Self-Regulation: Role and Use in Supporting Consumer Interests*, OECD Digital Economy Papers, No. 247 (Paris, 2015), p. 5.

**CASE STUDY. SUSPECT IDENTIFICATION IN BELGIUM**

As explained in chapter 1, an IP address is needed to connect a device to the Internet. Since the 1980s, the Internet Protocol version 4 standard (IPv4) has been used to allocate IP addresses. The IPv4 addressing system has, however, a finite number of IP addresses (equal to  $2^{32}$ , or approximately 4.29 billion addresses) which are running out. Unallocated IPv4 addresses ran out in Europe in 2019.<sup>a</sup> In addition to the adoption of Internet Protocol version 6 (IPv6), which has a much larger limit of addresses in comparison to IPv4, some Internet access providers have started to use a technology called carrier-grade network address translation (CGNAT) as an interim solution to the shortage of IPv4 addresses. CGNAT permits multiple end users to share one IP address. IP addresses are, however, a key way for law enforcement authorities to identify suspects online. Accordingly, the use of this technology to allow multiple end users to share a single IP address presents a potential barrier to the identification of suspects. Law enforcement authorities have expressed concerns about the growing use of this technology.<sup>b</sup>

In Belgium, cooperation between law enforcement authorities and Internet access providers has led to an informal agreement whereby Internet access providers would voluntarily restrict the maximum number of users using a single IP address to 16 before transitioning to IPv6. This solution represented a compromise between Internet access providers and industry to minimize interference with law enforcement investigations while ensuring user access to the Internet. This solution was reached without changing safeguards for access to personal data by law enforcement authorities and without legislative changes. It also did not require additional resources to be deployed by intermediaries.

<sup>a</sup> See further, RIPE Network Coordination Centre “The RIPE NCC has run out of IPv4 addresses”, 25 November 2019.

<sup>b</sup> See European Union Agency for Law Enforcement Cooperation (Europol), “Closing the online crime attribution gap: European law enforcement tackles Carrier-Grade NAT (CGN)”, press release, 2 February 2017; Europol, “Are you sharing the same IP address as a criminal? Law enforcement call for the end of Carrier Grade NAT (CGN) to increase accountability online”, press release, 17 October 2017.

**LIABILITY-BASED MEASURES**

Whereas cooperation-based measures seek to have industry cooperate with law enforcement authorities to prevent and combat illicit activity online through non-coercive means, States may also seek to prevent and combat illicit activity online through defining or circumscribing circumstances in which intermediaries may be held liable in relation to illicit activities occurring over their services. Liability refers to the imposition by the State, through generally-applicable legislation, of legal responsibility for taking or failing to take certain actions.<sup>96</sup> The purpose of holding online intermediaries legally responsible for crimes committed using their services is to deter conduct which could facilitate the commission of these crimes and hence incentivize online intermediaries to take steps to prevent and combat the commission of these crimes. Liability-based measures are one of, but not the only, means of achieving this end.

There are two broad approaches that States may take in determining the conditions under which online intermediaries may be liable in relation to wrongful conduct occurring over their services. The first is through rules that establish circumstances in which online intermediaries (whether designated as such, or as members of a broader class of actors) will be liable. Liability in this context may be criminal, civil or administrative. The second approach is through rules which define circumstances in which online intermediaries will not be liable. Likewise, these rules may provide immunity from criminal, civil and/or administrative liability. Provisions establishing such rules are known as non-liability provisions or safe-harbour provisions.

<sup>96</sup> See Jaani Riordan, “A theoretical taxonomy of intermediary liability”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 57 and 78.

Since the mid-1990s, legislative activity governing the conditions under which online intermediaries may be liable for wrongful conduct has been dominated by the introduction of non-liability provisions. Although online intermediaries, like all other natural and legal persons, are still subject to generally-applicable rules of criminal, tort and other liability, most States have tended to introduce rules establishing circumstances under which online intermediaries will be immune from liability, rather than creating new legal duties for online intermediaries and subjecting them to liability for breach.<sup>97</sup>

This section seeks to outline, with reference to relevant examples from national legislation, some of the key issues relating to liability-based approaches to preventing and combating wildlife crime, falsified medical products-related crime and trafficking in cultural property committed through online intermediaries. While legislative activity has favoured the introduction of non-liability provisions, this chapter first examines those rules which establish liability before considering those which provide immunity.

## Liability rules

Rules that set out circumstances in which online intermediaries will be liable vary in a number of ways. They may be special duties that apply to online intermediaries or a class thereof (such as duties to retain data or report to authorities) or they may be duties that are generally applicable to natural and legal persons (such as general principles of criminal liability and duties under the law of torts). They may involve primary liability, in the sense that liability is (or at least may be) based solely on the intermediary's own acts or omissions, or secondary liability, in the sense that liability requires at least *prima facie* proof of wrongdoing by a third party.<sup>98</sup> They may entail criminal, civil or administrative liability. They may involve a variety of different physical elements and may also vary according to the applicable mental elements.

Rules which establish liability for online intermediaries relevant to wildlife crime, falsified medical products-related crime or trafficking in cultural property online can be broadly categorized into two types. The first category are rules of secondary and inchoate liability for primary offences. The second are rules establishing offences for breach of statutory duties. Rules of secondary and inchoate liability are typically generally applicable – that is to say, they are not specifically targeted at online intermediaries – whereas the statutory duties of relevance to this topic are duties that are specific to online intermediaries. This paper examines both types of rules in turn.

### *Secondary and inchoate liability for primary offences*

Online intermediaries may be found directly liable for involvement in offences concerning wildlife crime, falsified medical products-related crime or trafficking in cultural property. In unusual cases, this may be for the commission of these offences themselves, in which case the intermediary can no longer be said to be acting as an intermediary but rather as the primary or principal offender. More likely to be relevant to online intermediaries are principles of secondary and inchoate liability.

<sup>97</sup> Dinwoodie, “A comparative analysis of the secondary liability of online service providers”, pp. 1, 19 and 31.

<sup>98</sup> Riordan, “A theoretical taxonomy of intermediary liability”, pp. 57, 63–65.



## Secondary liability

While the term may have different meanings under different legal systems,<sup>99</sup> for the purposes of this issue paper, secondary liability refers to situations where establishing liability requires at least *prima facie* proof of wrongdoing by a third party.<sup>100</sup> It is to be distinguished from primary liability, which may be based entirely on the acts or omissions of a single principal offender. Forms of secondary liability which may be relevant to online intermediaries in the context of this paper include aiding, abetting, counselling, procuring or facilitating the commission of an offence of wildlife crime, falsified medical products-related crime or trafficking in cultural property.

Secondary liability generally requires a higher degree of fault than that required for primary offending. This is because, “as the form of criminal liability moves further away from the actual infliction of harm, the grounds of liability should become narrower”.<sup>101</sup> Accordingly, aiding, abetting, counselling, procuring or facilitating the commission of an offence requires proof of intention – that the person intended the act of assistance or encouragement and knew that the principal offender intended or contemplated doing actions which constitute the offence.<sup>102</sup>

As regards secondary liability, it may be noted that article 5(1)(b) of the Organized Crime Convention requires that States parties establish criminal offences for, *inter alia*, intentionally “aiding, abetting, facilitating or counselling” the commission of serious crimes involving an organized criminal group. As noted in chapter 1, wildlife crime, falsified medical products-related crime, and trafficking in cultural property are of sufficient gravity to warrant penalties meeting the definition of “serious crime”.

An online intermediary could be guilty of aiding or abetting the commission of one of these crimes where they provide a service to a user, intending or knowing that that user would use the service to commit such an offence. An online intermediary could likewise be guilty of counselling, procuring or facilitating the commission of an offence if they could be proven to have designed or marketed a product with this intent. The case of Phantom Secure, outlined in the following section, involved a rogue online intermediary that designed and marketed an encrypted messaging service for the purpose of facilitating, *inter alia*, drug trafficking. The defendant in this case was charged with conspiracy to aid and abet the distribution of cocaine, though this charge was subsequently dropped pursuant to a plea agreement.

Provisions that establish secondary liability for wildlife crime, falsified medical products-related crime and trafficking in cultural property online may be found in criminal codes, criminal legislation specifically addressing these crime types, or legislation concerning cyber-enabled crimes. Section 113 of the Electronic Transactions Act, 2008 of Ghana is an example of the last approach. It expressly extends the abetment provisions of the Criminal Offences Act, 1960 to abetment wholly or partially effected through an electronic medium or an electronic agent.

<sup>99</sup> See Dinwoodie, “A comparative analysis of the secondary liability of online service providers”, pp. 1 and 8.

<sup>100</sup> See Riordan, “A theoretical taxonomy of intermediary liability”, pp. 57, 63–65.

<sup>101</sup> Andrew Ashworth and Jeremy Horder, *Principles of Criminal Law*, 7th ed. (Oxford, Oxford University Press, 2013), p. 432.

<sup>102</sup> A. P. Simester and others, *Simester and Sullivan’s Criminal Law: Theory and Doctrine*, 6th ed. (Oxford, United Kingdom, Hart Publishing, 2016), pp. 228–229 and 240; Ashworth and J. Horder, *Principles of Criminal Law*, pp. 431–432.

### EXAMPLE: GHANA – *ELECTRONIC TRANSACTIONS ACT, 2008*

#### Aiding and abetting

112. Sections 20 and 21 of the Criminal Offences Act, 1960 (Act 29) on abetment of crime applies with the necessary modification to any person who abets a crime whether the medium used in whole or in part was an electronic medium or an electronic agent.

### EXAMPLE: GHANA – *CRIMINAL OFFENCES ACT, 1960*

#### Section 20—Abetment of Crime and Trial and Punishment of Abettor.

- (1) Every person who, directly or indirectly, instigates, commands, counsels, procures, solicits, or in any manner purposely aids, facilitates, encourages, or promotes, whether by his act or presence or otherwise, and every person who does any act for the purpose of aiding, facilitating, encouraging or promoting the commission of a crime by any other person, whether known or unknown, certain or uncertain, is guilty of abetting that crime, and of abetting the other person in respect of that crime. [...]

*Note:* Section 147(1) of the *Companies Act, 2019* (Ghana) provides that companies shall be criminally liable for their acts “to the same extent as if the company were a natural person”.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

#### Inchoate liability

Inchoate liability refers to forms of liability that may arise before, or even without, the commission of any substantive offence.<sup>103</sup> While there are multiple forms of inchoate liability, such as incitement and attempt, the form of greatest relevance to online intermediaries is conspiracy. Conspiracy refers to the agreement of two or more persons to commit a criminal offence.<sup>104</sup> The mental elements of conspiracy are intention and knowledge.<sup>105</sup>

Article 5(1)(a) of the Organized Crime Convention requires that States parties criminalize participation in an organized criminal group and, as one possibility for doing so, to establish liability for conspiracy, in addition or as an alternative to the offence of criminal association. For the purposes of the Organized Crime Convention, conspiracy is understood as:

Agreeing with one or more other persons to commit a serious crime for a purpose relating directly or indirectly to the obtaining of a financial or other material benefit and, where required by domestic law, involving an act undertaken by one of the participants in furtherance of the agreement or involving an organized criminal group.<sup>106</sup>

<sup>103</sup> Simester and others, *Simester and Sullivan's Criminal Law*, p. 291.

<sup>104</sup> *Ibid.*, p. 310; Ashworth and Horder, *Principles of Criminal Law*, p. 467.

<sup>105</sup> Ashworth and Horder, *Principles of Criminal Law*, pp. 474–475; Simester and others, *Simester and Sullivan's Criminal Law*, p. 331.

<sup>106</sup> Organized Crime Convention, art. 5, para. 1 (a) (i).

Offences of conspiracy may be relevant where an online intermediary enters into an agreement with one or more other persons to provide services for the purposes of committing offences relating to wildlife crime, falsified medical products-related crime or trafficking in cultural property. It is important to note in this context that where it is the case that an online intermediary provides its services with the specific intention of facilitating illegal activity, it is no longer operating under the same “logic and incentive structure”<sup>107</sup> to the vast majority of law-abiding online intermediaries.

As with secondary liability, provisions that establish inchoate liability for wildlife crime, falsified medical products-related crime and trafficking in cultural property online may be found in criminal codes, criminal legislation specifically addressing these crime types, or legislation concerning cyber-enabled crimes.

### CASE STUDY. PHANTOM SECURE

The Canada-based company Phantom Secure provided hosting and instant messaging services as an online intermediary. Phantom Secure sold modified BlackBerry mobile phones and operated an encrypted network that allowed its devices to send and receive encrypted messages. Phantom Secure users paid approximately \$2,000–3,000 per six-month subscription for access to the handsets and the encrypted network. The founder and CEO, Mr Vincent Ramos, advertised Phantom Secure products as impervious to decryption, wiretapping or legal third-party records requests. The devices’ traffic was routed through encrypted servers located in countries and jurisdictions believed by Phantom Secure to be uncooperative with law enforcement. In addition, the locations of encrypted servers of Phantom Secure were also disguised through multiple layers of virtual proxy networks (VPNs).

During a meeting with undercover United States law enforcement agents, Mr Ramos admitted that Phantom Secure services were specifically designed for the purpose of facilitating drug trafficking. As part of the service it offered clients, Phantom Secure routinely deleted and destroyed evidence from devices that it knew had been seized by law enforcement. Indeed, it guaranteed that clients’ messages would be remotely deleted if the device was seized by law enforcement or otherwise became compromised. Furthermore, Phantom Secure did not sell its devices to the general public but operated on an exclusive referrals basis in order to prevent law enforcement from penetrating the Phantom Secure network.

Clearly, the activities of Phantom Secure went far beyond those of ordinary online intermediaries. As a result of Phantom Secure’s knowledge of the illicit activities of its clients and its intention to further such illicit activities, Mr Ramos and four other co-conspirators were charged with participating in a racketeering conspiracy to conduct enterprise affairs and with conspiracy to aid and abet the distribution of cocaine. The pattern of racketeering activity on which the racketeering conspiracy charges were laid included distribution of narcotics, importation of controlled substances, conspiracy to aid and abet the importation and distribution of controlled substances and obstruction of justice. As part of a plea deal, Mr Ramos pleaded guilty to the racketeering conspiracy charge and the charge of conspiracy to aid and abet the distribution of cocaine was dropped. He was sentenced to nine years’ imprisonment.

Further information about this case study is available on the UNODC knowledge management portal Sharing Electronic Resources and Laws on Crime (SHERLOC) case law database.<sup>b</sup>

<sup>a</sup> European Commission, *Hosting Intermediary Services and Illegal Content Online*, pp. 24–25.

<sup>b</sup> UNODC, Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal, Case law database, *United States of America v. Ramos*, Case No. USAx154, available at <https://sherloc.unodc.org/>

<sup>107</sup> European Commission, *Hosting Intermediary Services and Illegal Content Online*, pp. 24–25.

### *Liability for breach of statutory duty*

An additional source of potential liability for online intermediaries is liability for breach of statutory duties imposed on online intermediaries by the legislature. Unlike rules which establish secondary and inchoate liability, these provisions are specifically addressed at online intermediaries.

The types of statutory duties that online intermediaries may be subject to vary between jurisdictions. What they have in common is that these statutory duties attempt to provide online intermediaries with incentives to prevent and combat illicit activity online. Legislation regulating online intermediaries may establish, under penalty of liability, duties to remove or disable access to content,<sup>108</sup> to retain data,<sup>109</sup> to report knowledge of unlawful content to relevant authorities,<sup>110</sup> to disclose information requested by or otherwise render assistance to a law enforcement agency,<sup>111</sup> or to refrain from disclosing that an order (such as a preservation or production order) was made and that any action was taken or data collected under the order.<sup>112</sup> Where legislation establishes liability for failure to cooperate with law enforcement authorities in specified circumstances, these arrangements can be seen as a combination of cooperation- and liability-based measures. Duties to provide law enforcement authorities with information relating to unlawful content seek to address the problem of the removal of unlawful content potentially interfering with law enforcement investigations.

Section 3 of the German *Netzwerkdurchsetzungsgesetz* (known as “NetzDG”), set out below, which applies to social media providers operating for profit-making purposes and which have two million or more registered users in Germany,<sup>113</sup> provides that social media providers must maintain an effective and transparent procedure for handling complaints about unlawful content in accordance with several statutory requirements. This includes removing or blocking access to unlawful content within specified periods and retaining such content as evidence for a period of ten weeks.<sup>114</sup> A social media provider that intentionally or negligently fails to provide such a procedure commits a regulatory offence punishable by a fine of up to EUR 5 million.<sup>115</sup>

As with other policy measures where States establish liability for breach of statutory duties, it is critical that these measures be designed to provide online intermediaries with appropriate incentives to take effective and proportionate action against illicit content and activities. Liability for breach of statutory duty should not incentivize online intermediaries to remove legitimate content or block legitimate activities.

<sup>108</sup> See, for example, Computer Crime Proclamation of Ethiopia, art. 16.

<sup>109</sup> See, for example, Germany, Network Enforcement Act (NetzDG), sect. 3, para. 4 and sect. 4.

<sup>110</sup> See, for example, Electronic Transactions Act 2015 of Saint Vincent and the Grenadines, sect. 34, para. 2.

<sup>111</sup> See, for example, Cybercrime Act 2014 of Nigeria, sect. 23; Telecommunications Act 1997 (Cth) of Australia, sects. 317ZA–317ZB.

<sup>112</sup> See, for example, Electronic Crimes Act of Grenada, sect. 28, para. 2.

<sup>113</sup> Germany, Network Enforcement Act (NetzDG), sect. 1.

<sup>114</sup> Ibid., sect. 3, para. 2.

<sup>115</sup> Ibid., sect. 4.

### EXAMPLE: GERMANY – NETWORK ENFORCEMENT LAW (NETZWERKDURCHSETZUNGSGESETZ)<sup>a</sup>

#### Section 3

##### Handling of complaints about unlawful content

(1) The provider of a social network shall maintain an effective and transparent procedure for handling complaints about unlawful content in accordance with subsections (2) and (3). The provider shall supply users a procedure for submitting complaints about unlawful content that is easily recognisable while viewing the content, directly accessible, easy to use and permanently available.

(2) The procedure shall ensure that the provider of the social network:

1. takes immediate note of the complaint and checks whether the content reported in the complaint is unlawful and subject to removal or whether access to the content must be blocked,

2. removes or blocks access to content that is manifestly unlawful within 24 hours of receiving the complaint; this shall not apply if the social network has reached agreement with the competent law enforcement authority on a longer period for deleting or blocking any manifestly unlawful content,

3. removes or blocks access to all unlawful content immediately, this generally being within 7 days of receiving the complaint; the 7-day time limit may be exceeded if

- a) the decision regarding the unlawfulness of the content is dependent on the falsity of a factual allegation or is clearly dependent on other factual circumstances; in such cases, the social network can give the user an opportunity to respond to the complaint before the decision is rendered;
- b) the social network provider refers the decision regarding unlawfulness to a recognised self-regulation institution pursuant to subsections (6) to (8) within 7 days of receiving the complaint and agrees to accept the decision of that institution,

4. in the event of removal, secures the content for evidence and for this purpose saves it for a period of ten weeks within the scope of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1) and Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, p. 1; L 263, 6.10.2010, p. 15) as amended by Directive (EU) 2018/1808 (OJ L 303, 28.11.2018, p. 69),

5. to inform the complainant and the user for whom the contested content was stored about each decision without delay, and in doing so

- a) justifies his decision,
- b) indicates the possibility of an appeal as per § 3b(1) sentence 2, the procedure provided for this as per § 3b(1) sentence 3, the deadline as per § 3b(1) sentence 2 and that the content of the appeal can be passed on within the scope of the procedure as per § 3b(2)(1), and
- c) informs the complainant that he can file a notice of an offence and, if necessary, an application for prosecution against the user for whom the contested content has been saved, and about the website on which he can receive further information about this.

In the cases of sentence 1(3)(b), the social network provider may disclose the contested content, information on the time of sharing or making the content accessible and the extent of its dissemination, as well as the content in a recognisable context (if necessary for the purpose of the decision) to the recognised self-regulation body. The self-regulation body is authorised to process the personal data concerned to the extent necessary for the review. Any inaccuracy of the decision taken by the self-regulation body in the cases of sentence 1(3)(b) does not constitute a violation of paragraph 1, sentence 1 by the social network provider.



(3) The procedure shall ensure that each complaint, along with the measure taken to redress the situation, is documented within the scope of Directives 2000/31/EC and 2010/13/EU.

[...]

#### Section 4

##### Provisions on regulatory fines

(1) A regulatory offence shall be deemed to have been committed by any person who, intentionally or negligently,

[...]

2. in contravention of section 3(1) sentence 1, fails to provide, to provide correctly or to provide completely, a procedure mentioned therein for dealing with complaints submitted by complaints bodies or by users whose place of residence or seat is located in the Federal Republic of Germany,

[...]

(2) In cases under subsection (1) numbers 7 and 8, the regulatory offence may be sanctioned with a regulatory fine of up to five hundred thousand euros, and in other cases under subsection (1) with a regulatory fine of up to five million euros. Section 30(2) sentence 3 of the Act on Regulatory Offences shall apply.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

<sup>a</sup>English translation provided by the German Federal Ministry of Justice and Consumer Protection, Act to improve enforcement of the law in social networks (Network Enforcement Act, available at [www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG\\_node.html](http://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html)).

## LIABILITY OF LEGAL PERSONS

Both natural and legal persons may be subject to liability. Whereas natural persons are human beings, legal persons are businesses or organizations regarded as having personhood for the purposes of the law. Most online intermediaries will be legal persons, rather than natural persons.

Article 10(1) of the Organized Crime Convention provides that States parties to the Convention shall adopt such measures as may be necessary, consistent with their legal principles, to establish the liability of legal persons for participation in serious crime involving an organized criminal group and for the offences established in accordance with the Convention (participation in an organized criminal group, money-laundering, corruption and obstruction of justice). Both these types of offences could potentially be relevant to online intermediaries in the context of wildlife crime, falsified medical products-related crime and trafficking in cultural property. Article 10(2) of the Convention expressly provides that liability of legal persons may be criminal, civil or administrative.

Laws aimed at establishing liability for online intermediaries should also cover the liability of natural persons. Natural persons may be implicated in offences committed by legal persons operating as online intermediaries by virtue of their position and conduct within these businesses. Additionally, while the vast majority of relevant online intermediaries are legal persons, natural persons may also operate as online intermediaries, when self-employed or operating as sole traders, for example. Article 10(3) of the Organized Crime Convention provides that liability of legal persons shall be without prejudice to the criminal liability of natural persons who have

committed the offences in question. Policymakers therefore need to ensure that any offences established to address the conduct of online intermediaries in relation to wildlife crime, falsified medical products-related crime and trafficking in cultural property cover legal persons, as well as natural persons. This may need to be expressly provided for by legislation under the legal systems of some countries.

#### EXAMPLE: INDIA – THE INFORMATION TECHNOLOGY ACT, 2000

85. Offences by companies.—

- (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

- (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

*Explanation.*—

For the purposes of this section,—

- 1) “company” means any body corporate and includes a firm or other association of individuals; and
- 2) “director”, in relation to a firm, means a partner in the firm.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

## Non-liability rules

After the Internet first became a widespread tool for communication in the 1990s, legal cases concerning the liability of online intermediaries soon followed. These cases demonstrated the difficulties of striking a balanced solution for preventing and combating crime online, while also ensuring the growth of online services and the free exercise of the rights of the users of those services.

In France, the French subsidiary of a large United States-based online intermediary was ordered to prohibit French users from accessing postings displaying Nazi memorabilia on the parent company’s website.<sup>116</sup> A German court convicted the managing director of an Internet access provider for allowing the provider’s

<sup>116</sup>TGI de Paris, ordonnance de référé du 20 novembre 2000. See further *UEJF and Licra v. Yahoo! Inc and Yahoo France*, Case No. FRA001R, available at <https://sherloc.unodc.org/>.

network to be used to distribute child sexual abuse material.<sup>117</sup> On appeal, his conviction was overturned on the basis that, in the circumstances, it was not possible for his company to block or remove the material.<sup>118</sup> In Japan, a first instance court found the operators of an Internet access provider and the operator of an online forum liable for failure to remove defamatory comments hosted on the forum.<sup>119</sup> This decision was also subsequently overturned on appeal.<sup>120</sup>

These and other cases made it clear that the level of legal uncertainty concerning the liability of online intermediaries was unsustainable for all key stakeholders. Law enforcement agencies seeking to enforce the law needed to know what they could require of online intermediaries, intermediaries needed to have a clear understanding of the legal risks of providing online services, and Internet users needed legal certainty to make full use of the Internet's potential.

The solution for this uncertainty taken by legislators in many countries, starting in the mid-1990s, was to protect online intermediaries from liability for the illicit conduct of their users.<sup>121</sup> To do so, they introduced non-liability provisions (sometimes also known as safe-harbour provisions) into national legislation, establishing circumstances in which online intermediaries could not be held liable. So long as online intermediaries stayed within the safe harbours, they could conduct their business without fear of liability for the conduct of their users. In 1996, the United States introduced the Communications Decency Act which exempted online intermediaries from civil liability for the speech of their users.<sup>122</sup> This was followed by United States Digital Millennium Copyright Act in 1998, which established safe harbours for online intermediaries in relation to copyright infringement.<sup>123</sup> The year 2000 saw the introduction of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the "E-Commerce Directive"), which required Member States of the European Union to introduce legislation establishing particular safe harbours for online intermediaries.<sup>124</sup> Other States around the world followed, introducing similar non-liability provisions. Indeed, since the mid-1990s, the introduction of non-liability provisions has been the dominant trend in legislative activity addressing the conditions under which online intermediaries may be liable for wrongful conduct.<sup>125</sup> Most of these legislative regimes establish safe harbours for online intermediaries providing hosting, caching and "mere conduit" services.<sup>126</sup>

Although there are many similarities between the non-liability regimes that have been introduced around the world, there are also a number of ways in which they vary. These include whether the non-liability provisions are horizontal or vertical (in the sense of whether they apply to all forms of illicit activity or only some), whether they provide immunity from civil or criminal liability or both, the conditions for making use of the safe harbour, whether they expressly establish notice and takedown regimes and the nature of such regimes, whether they include Good Samaritan or non-monitoring provisions, and the effect of protection within the safe harbour. This section of the issue paper examines these non-liability rules in the context of this chapter's outline of rules governing online intermediaries' liability in relation to wildlife crime, falsified medical products-related crime and trafficking in cultural property committed online, and provides reference to relevant legislative examples.

<sup>117</sup> AG München, Urteil vom 28.05.1998 - 8340 Ds 465 Js 173158/95.

<sup>118</sup> LG München I, Urteil vom 17.11.1999 - 20 Ns 465 Js 173158/95. See further Lothar Determann, "Case update: German CompuServe director acquitted on appeal", *Hastings International and Comparative Law Review*, vol. 23, No. 1 (September 1999), p. 109.

<sup>119</sup> Niftyserve Gendai-Shiso Forum Case Decisions of Tokyo District Court on 26 May 1997 and Tokyo High Court on 5 September 2001.

<sup>120</sup> See further Hiroko Onishi, "The online defamation maze: are we finding a way out?", *International Review of Law, Computers & Technology*, vol. 27, Nos. 1 and 2 (March 2013), pp. 200, 202–204.

<sup>121</sup> See further Giancarlo F. Frosio, "Why keep a dog and bark yourself? From intermediary liability to responsibility", *Oxford International Journal of Law and Information Technology*, vol. 26, No. 1 (2018), pp. 1, 3–4.

<sup>122</sup> United States Code, Title 47, sect. 230.

<sup>123</sup> United States Code, Title 17, sect. 512.

<sup>124</sup> *Official Journal of the European Union*, L 178, 17 July 2000.

<sup>125</sup> Graeme B. Dinwoodie, "A comparative analysis of the secondary liability of online service providers", pp. 1, 19 and 31.

<sup>126</sup> Frosio, "Why keep a dog and bark yourself?", pp. 1 and 4.

### *Illicit activity of third parties covered*

Non-liability provisions may vary as to whether they protect online intermediaries from liability for all forms of illicit activity of their users (horizontal provisions) or only some (vertical provisions). Vertical regimes are common for matters such as copyright infringement and defamation but not for illicit trafficking online. All non-liability provisions covering liability for illicit trafficking online that were reviewed for the purposes of drafting this paper were horizontal in nature. In other words, none of the non-liability provisions reviewed for the purposes of drafting this paper expressly referred to illicit trafficking in wildlife products, falsified medical products or cultural property in defining the scope of applicable safe harbours.

#### **EXAMPLE: JAMAICA – ELECTRONIC TRANSACTIONS ACT**

##### **Liability of intermediaries**

25.— [...]

(2) An intermediary shall not be held liable in any civil or criminal proceedings for any information contained in an electronic document in respect of which the intermediary provides services, if the intermediary—

- (a) is not the originator of the document;
- (b) has no actual knowledge of the act or omission that gives rise to the civil or criminal liability, as the case may be, in respect of the document; and
- (c) has no knowledge of any facts or circumstances from which the likelihood of such civil or criminal liability ought reasonably to have been known.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

### *Type of liability protected from*

Non-liability provisions may also vary as to whether they exempt online intermediaries from both civil and criminal liability or only civil liability. Civil liability in this context refers to civil proceedings brought by private parties for damages or other civil remedies. Civil liability, in this sense of the term, is not covered by this paper. Section 25(2) of the Jamaican Electronic Transactions Act, set out in the preceding section, is an example of a non-liability provision that expressly covers both civil and criminal liability. The United States Communications Decency Act is an example of legislation which expressly excludes criminal liability from the protection of the safe harbour.

**EXAMPLE: UNITED STATES OF AMERICA – COMMUNICATIONS DECENCY ACT, 47 U.S.C. § 230**

**§ 230. Protection for private blocking and screening of offensive material**

[...]

**(e) Effect on other laws**

**(1) No effect on criminal law**

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

Some non-liability provisions do not expressly state the type of liability from which they provide protection. Article 14 of the European Union E-Commerce Directive, an excerpt of which is set out below, is an example of such a provision. Notwithstanding that it does not expressly state the types of liability from which it requires member States establish protections, article 14 is understood to provide protection against both civil and criminal liability.<sup>127</sup>

**EXAMPLE: EUROPEAN UNION – E-COMMERCE DIRECTIVE**

**Article 14**

**Hosting**

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

<sup>127</sup> European Commission, *Hosting Intermediary Services and Illegal Content Online*, p. 29.



### *Conditions for an online intermediary to avail itself of the safe harbour*

The conditions which an online intermediary must meet in order to avail itself of the safe harbour established by a non-liability provision also differ between jurisdictions and between legislative regimes within jurisdictions. Commonly, these conditions include conditions relating to the functions exercised by the online intermediary, conditions relating to its knowledge of the illicit content or activity and conditions relating to the conduct of the online intermediary upon obtaining knowledge of illicit content or activities. The following sections of this chapter consider each type of condition, with reference to relevant legislative examples.

#### **Conditions relating to the functions of the online intermediary**

Legislation establishing safe harbours for online intermediaries firstly limits the availability of protections from liability by defining the types of actors that can avail themselves of the safe harbour. These conditions relate to the functions that the online intermediary is exercising in relation to the alleged illegal activity. In the European Union, for example, liability exemptions exist for “mere conduit”, caching and hosting services.<sup>128</sup>

Conditions relating to the functions of the online intermediary may be expressly provided for in non-liability provisions or may be implicitly included in definitions of the types of intermediaries that can avail themselves of these provisions.<sup>129</sup> Typically these provisions require that the intermediary not be the “originator” of the data,<sup>130</sup> that the intermediary does not initiate the transmission, select its receiver or select or modify the information contained therein,<sup>131</sup> or that the conduct of the intermediary be of a “mere technical, automatic and passive nature”.<sup>132</sup> Hence, in many jurisdictions, one of the conditions for online intermediaries to avail themselves of non-liability provisions is that their conduct must have been “passive”, and not “active”, in respect of the data. Whether the conduct of an intermediary has been passive or active in respect of allegedly illicit activity can be a complex question and one that has been subject to judicial consideration in litigation against online intermediaries.<sup>133</sup>

#### **Conditions relating to the knowledge of the online intermediary**

Online intermediaries will typically lose the protection of a safe harbour if they have knowledge of an illegal activity occurring over its services and do not promptly take steps to remove or disable access to such content. In other words, to avail itself of the protection of the safe harbour, it is a condition that the online intermediary does not have knowledge of such illegal activity or, if it obtains such knowledge, that it promptly takes action to remove or disable access to the content in question. The key features of such conditions include the applicable standard of knowledge, what that knowledge must be of, how knowledge can be obtained on the part of the intermediary and the steps that the intermediary must take to retain the protection of the safe harbour upon obtaining such knowledge. These features are examined below.

##### **Standard of knowledge**

The relevant standard of knowledge which can lead to loss of the benefits of a safe harbour may be, depending on the legislative regime in question, actual or constructive knowledge. Actual knowledge is a subjective standard and involves an inquiry into the matters that were actually known by the intermediary in question. On the other hand, constructive knowledge incorporates objective considerations whereby an online intermediary may be taken to have knowledge of illegal activity if it was aware of facts or circumstances from

<sup>128</sup> E-Commerce Directive of the European Union, arts. 12–14.

<sup>129</sup> Dinwoodie, “A comparative analysis of the secondary liability of online service providers”, pp. 1 and 5.

<sup>130</sup> See, for example, Electronic Transactions Act of Barbados, sect. 23, para. 1.

<sup>131</sup> See, for example, India, Information Technology Act, 2000, sect. 79, para. 2.

<sup>132</sup> E-Commerce Directive of the European Union, preamble para. 42; *Google France SARL v. Louis Vuitton Malletier SA*, Cases No. 237–238/08, judgment of 23 March 2020, paras. 113–114; *L'Oréal SA v. eBay International AG*, Case No. C-324/09, judgment of 12 July 2011, para. 113.

<sup>133</sup> See, for example, *Google France SARL v. Louis Vuitton Malletier SA*; *L'Oréal SA v. eBay International AG*.

which knowledge of the illegal activity would have been reasonably apparent to a competent operator standing in its shoes.<sup>134</sup> Of the two, actual knowledge represents a higher standard and hence a narrower basis for loss of protection from liability.

In some jurisdictions, the applicable standard of knowledge depends on the type of liability. The hosting safe harbour in the European Union, set out on page 46, is an example of this. The higher standard of actual knowledge applies in respect of criminal liability, whereas constructive knowledge suffices in respect of civil liability for damages (that is, being “aware of facts or circumstances from which the illegal activity or information is apparent”).<sup>135</sup> Similar language is contained in the Malawian legislation, set out below.

#### EXAMPLE: MALAWI – ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016

##### Liability of an intermediary service provider

25.—(1) An intermediary service provider shall not be liable in any civil or criminal proceedings for any information contained in an electronic message in respect of which he provides services, if the intermediary service provider—

- (a) has not initiated the transmission of the message;
- (b) has no actual knowledge of the act or omission that gives rise to the civil or criminal liability as the case may be, in respect of the message; and
- (c) has no knowledge of any facts or circumstances from which the likelihood of such civil or criminal liability ought reasonably to have been known.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

##### Knowledge of what

A further legal issue concerns what the online intermediary must have “actual knowledge” or “awareness” of in order to avail themselves of the protection of the safe harbour. In the E-Commerce Directive of the European Union, the hosting safe harbour refers to “actual knowledge of illegal activity or information”. However, the provision is silent as to whether this requires general knowledge of the use of the intermediary’s service to host illicit content or rather knowledge of specific illicit content hosted by the intermediary. In general, European courts have interpreted “actual knowledge” as requiring knowledge of specific illicit content.<sup>136</sup> As regards the standard of awareness “of facts or circumstances from which the illegal activity or information is apparent” (that is, the standard of constructive knowledge applicable to civil claims for damages under the E-Commerce Directive), the Court of Justice of the European Union has held that this provision applies where an online intermediary is “aware of facts or circumstances on the basis of which a diligent economic operator should have realised” that particular activity or information was illegal.<sup>137</sup>

Whether activity or information is illegal can, however, be a difficult question for online intermediaries to answer. As noted by one commentator,

<sup>134</sup> Riordan, “A theoretical taxonomy of intermediary liability”, pp. 57 and 61.

<sup>135</sup> Aleksandra Kuczerawy, “Intermediary liability & freedom of expression: recent developments in the EU notice & action initiative”, *Computer Law & Security Review*, vol. 31, No. 1 (February 2015), pp. 46, 50–51.

<sup>136</sup> European Commission, *Hosting Intermediary Services and Illegal Content Online*, p. 38.

<sup>137</sup> *L’Oréal SA v. eBay International AG*, para. 124.

‘Knowledge’, in a substantive sense, requires more than mere awareness of potentially problematic content—it requires intermediaries to make a judgment about whether the material falls within the ambit of the relevant law. At the time that the intermediary is put on notice, it is usually only through an allegation of harm, and it is sometimes difficult for an intermediary to evaluate whether a claim is likely to be made out. In defamation, for example, this may require an evaluation of whether evidence of the truth of an imputation can be gathered; in copyright, the existence of a fair dealing defence or licence can be a difficult question of fact and law.<sup>138</sup>

Similar difficulties exist in relation to each of the three crime types covered by this paper. It may be difficult for online intermediaries to determine whether particular wildlife products are illicit, particular medical products are falsified, or particular cultural property is trafficked as these illicit goods may be indistinguishable or difficult to distinguish from licit goods and the legality or illegality of an act of sale, offering for sale, distribution, transportation, import, export and so on may depend on external circumstances.

How knowledge can be obtained

In practice, there may be a variety of ways that an online intermediary can obtain knowledge of illegal activity. Such knowledge may be obtained through a notice from a third party, a court order or the intermediary’s own investigations. Where a non-liability provision provides that protection from liability will be lost if the online intermediary has knowledge of illegal activity, it will ordinarily not be material *how* the online intermediary came to have this knowledge. In *L’Oréal SA v. eBay International AG*, the Court of Justice of the European Union held, in relation to the standard of constructive knowledge in article 14(1)(a) of the E-Commerce Directive:

if [such rules] are not to be rendered redundant, they must be interpreted as covering every situation in which the provider concerned becomes aware in one way or another of [facts or circumstances from which the illegal activity or information is apparent].

The situations thus covered include, in particular, that in which the operator of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information.<sup>139</sup>

Thus, under the E-Commerce Directive of the European Union, a host of material may be liable without ever having received a takedown notice.<sup>140</sup>

From the starting point that “knowledge” refers to knowledge howsoever required, some legislators and courts have modified this condition by setting out circumstances where an online intermediary will be deemed to have or not have knowledge of illegal activity or by setting out circumstances where proof of knowledge will not be required.

In some countries, legislators have established procedures for government organs or third parties to inform online intermediaries that their services are being used to commit an unlawful act. Where an online intermediary receives such a notice, non-liability provisions in a small number of countries provide that further proof of knowledge is not necessary. In Kenya, for example, s 56(1) of the Computer Misuse and Cybercrimes Act, 2018, set out below, expresses the requirements of “actual notice, actual knowledge, or willful and malicious intent” disjunctively, such that proof of actual knowledge is not necessary if an online intermediary has received “actual notice”. The Computer Misuse and Cybercrimes Act, 2018 does not, however, further define what constitutes “actual notice”. In India, s 79(3)(b) of The Information Technology Act, 2000 provides that the safe harbour in s 79(1) shall not apply if, “upon receiving actual knowledge, or on being notified by the

<sup>138</sup> Kylie Pappalardo and Nicolas Suzor, “The liability of Australian online intermediaries”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 236, 248–249 (citations omitted).

<sup>139</sup> *L’Oréal SA v. eBay International AG*, paras. 121–122.

<sup>140</sup> Eric Goldman, “An overview of the United States’ section 230 Internet immunity”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 155 and 168.

appropriate Government or its agency”, the intermediary fails to take certain steps. Again, the disjunctive expression of this provision establishes notice from the government as an alternative to proof of actual knowledge.

#### EXAMPLE: KENYA – COMPUTER MISUSE AND CYBERCRIMES ACT, 2018

##### Confidentiality and limitation of liability

56. (1) A service provider shall not be subject to any civil or criminal liability, unless it is established that the service provider had actual notice, actual knowledge, or willful and malicious intent, and not merely through omission or failure to act, had thereby facilitated, aided or abetted the use by any person of any computer system controlled or managed by a service provider in connection with a contravention of this Act or any other written law.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

#### EXAMPLE: INDIA – THE INFORMATION TECHNOLOGY ACT, 2000

##### 79. Exemption from liability of intermediary in certain cases.—

- (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
- (2) The provisions of sub-section (1) shall apply if—
  - (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
  - (b) the intermediary does not—
    - (i) initiate the transmission,
    - (ii) select the receiver of the transmission, and
    - (iii) select or modify the information contained in the transmission;
  - (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
- (3) The provisions of sub-section (1) shall not apply if—
  - (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
  - (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

*Explanation.*—For the purposes of this section, the expression “third party information” means any information dealt with by an intermediary in his capacity as an intermediary.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

An alternative means of achieving a similar result is for legislators to provide that knowledge of certain facts is presumed when an online intermediary receives notice of particular matters. This is the case in France, for example, under *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, article 6 I.-5 of which provides that knowledge of the manifestly illegal character of certain activity or information can be presumed to have been acquired by online intermediaries if they receive notice of the description and location of the content in question, the legal basis for removing or disabling access to it, the name and contact information of the notifier and, except as regards certain serious crimes, a copy of correspondence addressed to the author or publisher of the information or activities in question demanding their discontinuation, removal or modification or a justification that the author or publisher could not be contacted. An excerpt of article 6 is set out below.

#### EXAMPLE: FRANCE – ACT NO. 2004-575 OF 21 JUNE 2004 ON CONFIDENCE IN THE DIGITAL ECONOMY

##### Article 6

I.

[...]

2. Natural or legal persons who, whether or not for a fee, store signals, written texts, images, sound files or messages of any kind provided by users of online public communication services, for the purpose of making those data available to the public through such services, cannot be held civilly liable for such activities or information stored at the request of a user of those services if said persons were effectively unaware of the manifestly illegal nature of the activities or information or of facts or circumstances revealing that nature, or if, upon becoming aware thereof, they acted promptly to remove the data or make them inaccessible.

The preceding subparagraph does not apply when the user of the service is acting under the authority or control of a natural or legal person as referred to in that subparagraph.

3. The persons referred to in paragraph 2 cannot be held criminally liable for the information stored at the request of a user of such services if they were effectively unaware of the manifestly illegal nature of the activity or information or if, upon becoming aware of that nature, they acted promptly to remove the information or make it inaccessible.

The preceding subparagraph does not apply when the user of the service is acting under the authority or control of a natural or legal person as referred to in that subparagraph.

[...]

5. The persons referred to in paragraph 2 are presumed to be aware of the illegal content when they have been notified of the following:

If the notifier is a natural person: surname, first name and email address; if the notifier is a legal person: corporate form, company name and email address; and if the notifier is an administrative authority: name and email address. These conditions are deemed to be met if the notifier is a registered user of the online public communication service as referred to in paragraph 2, if the notifier is online at the time of notification and if the operator has collected the information needed in order to identify the notifier.

A description of the illegal content, its exact location and, where applicable, the electronic address(es) at which it can be accessed. These conditions are deemed to be met if the online public communication service as referred to in paragraph 2 allows such notification to be made by means of a mechanism that is directly accessible from within the illegal content.



The legal grounds on which the illegal content should be removed or made inaccessible. This condition is deemed to be met if the online public communication service as referred to in paragraph 2 allows notification to be made by means of a mechanism capable of indicating the category of offence to which the illegal content relates.

A copy of the correspondence addressed to the author or publisher of the illegal information or activities requesting that the information or activities be suspended, removed or modified, or evidence that the author or publisher could not be contacted. This condition is not a requirement for notification of the offences referred to in the third subparagraph of paragraph 7 of the present section I and in article 24 bis and the third and fourth paragraphs of article 33 of the Act of 29 July 1881 on freedom of the press.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

Legislation or judicial decisions can also limit the circumstances in which an online intermediary can be considered to have obtained knowledge of illicit activity. Though it does not apply to criminal liability and is instead limited to civil liability for copyright infringement, section 193D(3) of the Copyright Act of Singapore provides a concise example of such a provision. Section 193D(3) provides that if a notice is not made in a prescribed manner, in or substantially in accordance with, the prescribed form, and stating certain prescribed matters, it shall not be considered in determining whether the online intermediary had knowledge of the alleged infringement.

#### EXAMPLE: SINGAPORE — COPYRIGHT ACT (CAP 63)

##### Storage and information location

193D.— [...]

(3) For the purposes of subsection (2), a notice purportedly made by the owner of the copyright in the material or under the owner's authority which is not a notice referred to in subsection (2)(b)(iii), or a notice under section 193DDB(1)(b), shall not be considered in determining whether the network service provider has acquired any knowledge referred to in subsection (2)(b)(i) or (ii).

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

In the case of *Shreya Singhal v. Union of India*, the Supreme Court of India also ruled that “actual knowledge”, for the purposes of s 79(3)(b) of The Information Technology Act, 2000, set out on page 50, can only be obtained through a court order.<sup>141</sup> The Supreme Court of India's reading down of s 79 in this case appears to have been influenced by its interpretation of the provision as liability-imposing, and not merely liability-exempting.<sup>142</sup>

<sup>141</sup> *Shreya Singhal v. Union of India*, judgment of 24 March 2015, para. 117.

<sup>142</sup> Kyung-Sin Park, “From liability trap to the world's safest harbour: lessons from China, India, Japan, South Korea, Indonesia, and Malaysia”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 251, 261–263.

The interpretation of actual knowledge as requiring a court order is unusual as regards non-liability provisions worldwide and has the effect that online intermediaries in India enjoy the protection of one of the world's broadest safe harbours.<sup>143</sup>

#### Conditions relating to conduct of the online intermediary upon obtaining knowledge

An online intermediary will not automatically lose the protection of a safe harbour if they obtain knowledge of illegal activity occurring over their services. If an online intermediary obtains such knowledge, they will generally not lose the protection of the safe harbour if they act quickly to remove or disable access to such content.

In some countries, non-liability provisions also require that the online intermediary notify the appropriate law enforcement agency of the illegal activity to retain the protection of the safe harbour and/or preserve data as evidence of the illegal activity. States establishing such approaches should ensure that both the circumstances in which reports must be made to law enforcement agencies and the content of such reports are proportionate to the policy goals in question to ensure, inter alia, respect for users' privacy. Non-liability provisions may also provide that access to a safe harbour is contingent upon following a procedure set out in an applicable code of conduct developed by industry and approved by the relevant government minister. Each of these obligations may also be established independently of access to a safe harbour. In other words, it is one question whether legislation subjects online intermediaries to these duties; it is another whether failure to comply with these duties will result in the loss of the protections of a safe harbour.

#### EXAMPLE: TRINIDAD AND TOBAGO – ELECTRONIC TRANSACTIONS ACT

Liability of intermediaries and telecommunications service providers.

50. (1) An intermediary or telecommunications service provider who merely provides a conduit for the transmission of data messages, records or information in electronic form shall not be liable for the content of data messages, records or information in electronic form if the intermediary or telecommunications service provider has no actual knowledge or is not aware of facts that would to a reasonable person, indicate a likelihood of criminal liability or liability for a tort in respect of material on the network of an intermediary or telecommunications service provider or who, upon acquiring actual knowledge or becoming aware of such facts, follows the procedures required by section 51.

[...]

Procedure for dealing with unlawful, defamatory, etc., information.

51. (1) If an intermediary or telecommunications service provider has actual knowledge that the information in a data message or an electronic record gives rise to civil or criminal liability then, as soon as is practicable after acquiring such knowledge, the intermediary or telecommunications service provider shall—

- (a) remove and secure the information from any information system within the control of the intermediary or telecommunications service provider and cease to provide or offer to provide services in respect of that information or take any other action authorised by written law or in accordance with the established code of conduct; and
- (b) in the case of criminal liability, notify the appropriate law enforcement authority of the relevant facts and of the identity of the person for whom the intermediary or telecommunications service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary or telecommunications service provider.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

<sup>143</sup> Ibid., pp. 251, 259 and 263.

### EXAMPLE: ESTONIA – INFORMATION SOCIETY SERVICES ACT

#### § 11. No obligation to monitor

[...]

(3) Service providers are required to promptly inform the competent supervisory authorities of alleged illegal activities undertaken or information provided by recipients of their services specified in §§ 8–10 of this Act, and to communicate to the competent authorities information enabling the identification of recipients of their service with whom they have storage agreements.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

### EXAMPLE: MALAWI – ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016

#### Saving of data

29.—(1) An intermediary service provider shall, while exercising the activities prescribed in section 30, maintain and preserve the data that permits the identification of any person who contributed to the creation of all or part of the content relating to the services rendered by such intermediary service provider.

(2) The High Court may require from the intermediary service provider communication of the data referred to in subsection (1).

(3) The Authority may issue regulations governing the retention of data referred to in this section.

#### Takedown notification

30.—[...]

(2) An intermediary service provider shall set up an easily accessible and visible system to enable any person inform the intermediary service provider of any content which is unlawful or infringes, or may infringe, on such person's rights.

(3) An intermediary service provider shall—

- (a) inform promptly the Authority or its organs of any illegal content reported as indicated in subsection (2) and made available online by the beneficiaries of their services; and
- (b) make public the means taken to fight against the dissemination of such illegal content.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

**EXAMPLE: SOUTH AFRICA – ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002****Recognition of representative body**

71. (1) The Minister may, on application by an industry representative body for service providers by notice in the Gazette, recognise such body for purposes of section 72.

(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister that—

- (a) its members are subject to a code of conduct;
- (b) membership is subject to adequate criteria;
- (c) the code of conduct requires continued adherence to adequate standards of
- (d) the representative body is capable of monitoring and enforcing its code of conduct; and conduct adequately.

**Conditions for eligibility**

72. The limitations on liability established by this Chapter apply to a service provider only if—

- (a) the service provider is a member of the representative body referred to in section 71; and
- (b) the service provider has adopted and implemented the official code of conduct of that representative body.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

**Notice and takedown regimes**

Notice and takedown regimes refer to mechanisms whereby an online intermediary (a) is provided notice that particular content or a particular activity in relation to which the intermediary provides a service is alleged to be in breach of the law; (b) is required to assess the legality of that content or activity; and (c) if such content or activity is assessed to be illegal, is obliged to remove or disable access to it or, in some cases, suspend the provision of services to the infringing user. Notice and takedown regimes may be expressly established by legislation or may simply be impliedly established through conditioning access to safe harbours on prompt action to remove or disable access upon obtaining knowledge of illicit activity. The latter is the case under the E-Commerce Directive of the European Union.<sup>144</sup> In some cases, notice and takedown systems have also been adopted by online intermediaries in the absence of legislative provisions requiring this.<sup>145</sup>

Where legislation expressly establishes a notice and takedown regime, it may include formal requirements for valid notice and establish time frames for particular actions involved in the notice and takedown procedure.<sup>146</sup> Legislative provisions establishing such matters can be advantageous as they provide online intermediaries with a greater measure of legal certainty as to what is required of them and hence lower the risk of

<sup>144</sup> See further Aleksandra Kuczerawy, “From ‘Notice and Takedown’ to ‘Notice and Stay Down’: risks and safeguards for freedom of expression”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford University Press, 2020), pp. 525 and 528.

<sup>145</sup> See further Dinwoodie, “A comparative analysis of the secondary liability of online service providers”, pp. 1 and 40.

<sup>146</sup> Kuczerawy, “From ‘Notice and Takedown’ to ‘Notice and Stay Down’”, pp. 525 and 530.

overcompliance with takedown requests.<sup>147</sup> However, even in such cases, the assessment of the legality of content is complex and often cannot be done with sufficient certainty. In other words, there remain significant incentives for overcompliance, in particular when combined with strict mandatory deadlines. This highlights the need for robust appeals and remedial processes as well as measures that prevent bad faith flagging of content. In some countries, notice and takedown regimes include penalties for takedown notices issued in bad faith.<sup>148</sup>

Rule 3(4) of the Indian Information Technology (Intermediaries Guidelines) Rules, 2011, set out below, sets out a time frame within which a hosting provider must act upon obtaining notice or otherwise obtaining knowledge of particular types of illicit content. It further requires that the intermediary preserve relevant information for a period of at least 90 days. Section 3 of the German NetzDG, an excerpt of which is set out on page 41, sets out time frames within which a social media provider to which the law applies must remove or block access to unlawful content. These time frames distinguish between “manifestly unlawful content” and other forms of unlawful content covered by the law. Article 6 I.-5 of the French *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique*, discussed above, sets out a number of requirements for effective notice, if knowledge of particular facts is to be presumed from the notice. Section 77(1) of the South African Electronic Communications and Transactions Act, 2002, set out below, also establishes a number of requirements for a takedown notice. The South African Act is, however, silent as to the effect of notice that does not comply with these formal requirements.<sup>149</sup>

#### EXAMPLE: SOUTH AFRICA – ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002

##### Take-down notification

77. (1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include—

- (a) the full names and address of the complainant;
- (b) the written or electronic signature of the complainant;
- (c) identification of the right that has allegedly been infringed;
- (d) identification of the material or activity that is claimed to be the subject of unlawful activity;
- (e) the remedial action required to be taken by the service provider in respect of the complaint;
- (f) telephonic and electronic contact details, if any, of the complainant;
- (g) a statement that the complainant is acting in good faith;
- (h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; [...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

<sup>147</sup> Ibid.; Dinwoodie, “A comparative analysis of the secondary liability of online service providers”, pp. 1 and 44.

<sup>148</sup> See, for example, Antigua and Barbuda, Electronic Transactions Act, 2013, sect. 34, para. 5; France, *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique*, art. 6 I.-4; Ghana, Electronic Transactions Act, 2011, sect. 31, para. 2.

<sup>149</sup> Nicolo Zingales, “Intermediary liability in Africa: looking back, moving forward?”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 214 and 217.



**EXAMPLE: INDIA – INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES, 2011****3. Due diligence to be observed by intermediary—**

The intermediary shall observe following due diligence while discharging his duties, namely:—

- (1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.
- (2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —
  - (a) belongs to another person and to which the user does not have any right to;
  - (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
  - (c) harm minors in any way;
  - (d) infringes any patent, trademark, copyright or other proprietary rights;
  - (e) violates any law for the time being in force;
  - (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
  - (g) impersonate another person;
  - (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
  - (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation

[...]

- (4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

A final mechanism relevant to notice and takedown regimes are “trusted notifier” or “trusted flagger” arrangements. Under such arrangements “a privileged notification channel is provided by an intermediary to a third party, which is particularly knowledgeable or has particular expertise to identify unlawful content”.<sup>150</sup> Depending on the arrangements in question, the trusted notifier could “range from individual or organized networks of private organizations, civil society organizations and semi-public bodies, to public

<sup>150</sup> Sebastian Felix Schwemer, “Trusted notifiers and the privatization of online”, *Computer Law & Security Review*, vol. 35, No. 6 (July 2019), p. 4.

authorities”.<sup>151</sup> Proponents of trusted notifier arrangements argue that, as a result of trusted notifiers’ knowledge or expertise and the reliance that online intermediaries can place on notifications received by trusted notifiers, these arrangements can result in “higher quality notices and faster take-downs”.<sup>152</sup> Trusted notifiers are one proposed remedy to the problem of online intermediaries having neither the competence nor resources to assess the legality of content.<sup>153</sup> At the same time, concerns have been expressed about the lack of accountability, representativeness of private bodies designated to be trusted flaggers, the lack of transparency as to their decision-making and the implications of these issues for the rule of law and the exercise of the right to due process online.<sup>154</sup> There is a further risk that online intermediaries delegate their responsibility for assessing the legality of content to trusted notifiers, “rubber-stamping” takedown notices and removing lawful content.<sup>155</sup> These concerns could be partly mitigated by legislative arrangements guaranteeing certain levels of transparency and procedural safeguards.<sup>156</sup>

### *Good Samaritan provisions*

Conditioning access to a safe harbour on an online intermediary not having knowledge of illicit activity disincentivizes online intermediaries from taking proactive steps to address illicit activity occurring over their services. This disincentive is compounded where access to a safe harbour is further conditioned on the conduct of an online intermediary being passive, rather than active.<sup>157</sup> Online intermediaries may be faced with a choice between actively taking steps to moderate or remove user content – but at the cost of accepting legal responsibility for any illicit content that they do not remove – or doing as little as possible to manage user content, thereby avoiding being characterized as being active in relation to the content or having actual or constructive knowledge about the content.<sup>158</sup> From the perspective of the online intermediary, this situation has been termed the “Moderator’s Dilemma”;<sup>159</sup> from the perspective of legislators seeking to prevent and combat the proliferation of illicit content online, this issue is known as the “Good Samaritan” problem.

Some States have taken steps to address the Good Samaritan problem through the introduction of provisions ensuring that the voluntary actions of online intermediaries taken in good faith to remove or disable access to illicit content do not give rise to liability on the part of the intermediaries. An early example of such a “Good Samaritan provision”, albeit one from the context of civil liability, is § 230(c) of the United States Communications Decency Act, an excerpt of which is set out below. Section 230(c)(2) provides both that online intermediaries shall not be liable on account of voluntary actions taken in good faith to remove or restrict access to or availability of content and that they shall not be liable “when they miss such content and do not take any action at all”.<sup>160</sup>

A variation of a Good Samaritan provision which is in some ways potentially narrower than that contained in the United States legislation is s 25(4) of the Electronic Transactions and Cyber Security Act, 2016 of Malawi. This provision applies to both civil and criminal liability and is set out below. Section 25(4) provides that “[an intermediary service provider shall not be liable for any act done in good faith pursuant to this section”. A

<sup>151</sup> Ibid.

<sup>152</sup> European Commission, “Tackling illegal content online: towards an enhanced responsibility of online platforms” (Brussels, 2017), p. 8.

<sup>153</sup> Schwemer, “Trusted notifiers and the privatization of online”.

<sup>154</sup> A/HRC/38/35, para. 34; Schwemer, “Trusted notifiers and the privatization of online”, p. 4.

<sup>155</sup> Ibid., p. 8.

<sup>156</sup> Ibid., p. 13.

<sup>157</sup> European Commission, *Hosting Intermediary Services and Illegal Content Online*, p. 39.

<sup>158</sup> Goldman, “An overview of the United States’ section 230 Internet immunity”, pp. 155 and 157; European Commission, *Hosting Intermediary Services And Illegal Content Online*, p. 41.

<sup>159</sup> See, for example, Goldman, “An overview of the United States’ section 230 Internet immunity”, pp. 155 and 157.

<sup>160</sup> Aleksandra Kuczerawy, “The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?”, KU Leuven Centre for IT and IP Law, 24 April 2018. See also European Commission, *Hosting Intermediary Services and Illegal Content Online*, p. 42. For an explanation of the background to sect. 230 (c) of the Communications Decency Act, see Benjamin C. Zipursky, “Online defamation, legal concepts, and the good Samaritan”, vol. 51, para. 1, *Valparaiso University Law Review* (2016), pp. 30–33.

similar provision is contained in the legislation of Jamaica.<sup>161</sup> Unlike the United States provision, which expressly refers to “any action *voluntarily taken* in good faith to restrict access to or availability of material”,<sup>162</sup> what constitutes an act “pursuant to” the provisions of the Malawian and Jamaican legislation may be less clear. In particular, it is not clear whether these provisions cover situations where an intermediary takes some steps to remove or disable access to certain illicit content but does not manage to remove all such content.

#### EXAMPLE: UNITED STATES OF AMERICA – 47 U.S.C. § 230

##### § 230. Protection for private blocking and screening of offensive material

[...]

##### (c) Protection for “Good Samaritan” blocking and screening of offensive material

[...]

##### (2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

#### EXAMPLE: MALAWI – ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016

##### Liability of an intermediary service provider

25.—(1) An intermediary service provider shall not be liable in any civil or criminal proceedings for any information contained in an electronic message in respect of which he provides services, if the intermediary service provider—

- (a) has not initiated the transmission of the message;
- (b) has no actual knowledge of the act or omission that gives rise to the civil or criminal liability as the case may be, in respect of the message; and
- (c) has no knowledge of any facts or circumstances from which the likelihood of such civil or criminal liability ought reasonably to have been known.

<sup>161</sup> Jamaica, Electronic Transactions Act, sect. 25, para. 5.

<sup>162</sup> United States Code, Title 47, sect. 230 (c)(2)(A) (emphasis added).

[...]

(3) If in relation to information contained in an electronic message in respect of which an intermediary service provider renders his services, the intermediary service provider has—

(a) actual knowledge of the act or omission that gives rise to civil or criminal liability, as the case may be, in respect of the message; or

(b) knowledge of any fact or circumstance from which the likelihood of such civil or criminal liability ought reasonably to have been known, he shall forthwith remove the document from any electronic communication system within his control and shall cease to provide services in relation to the message.

(4) An intermediary service provider shall not be liable for any act done in good faith pursuant to this section.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

While Good Samaritan provisions attempt to solve one problem relating to illicit content online, they have been criticized for creating other problems. In particular, Good Samaritan provisions have been criticized for failing to provide persons whose content is wrongly removed, but removed in good faith, with access to an effective remedy. Furthermore, Good Samaritan provisions have been criticized for encouraging excessive removal of content.<sup>163</sup>

### Non-monitoring provisions

While States sometimes wish to avoid providing disincentives for online intermediaries to take proactive steps to detect and remove illicit content, many States have also been careful not to impose upon online intermediaries a general obligation to monitor the content of their users, to avoid infringing upon the right to privacy and freedom of expression.<sup>164</sup> Many States have thus introduced “non-monitoring provisions” to this effect. Two examples of such provisions, from the E-Commerce Directive of the European Union and the Electronic Communications Act, 2009 of Zambia, are set out below.

#### EXAMPLE: EUROPEAN UNION – E-COMMERCE DIRECTIVE

##### Article 15

##### No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

<sup>163</sup> See, for example, Kuczerawy, “The EU Commission on voluntary monitoring”.

<sup>164</sup> A/HRC/38/35, para. 67; Council of Europe, Committee of Ministers, “Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities”.

**EXAMPLE: ZAMBIA – ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2009**

No general obligation on service provider to monitor unlawful activities

62. (1) Subject to the other provisions of this Part, a service provider shall not be under any obligation to—

- (a) monitor the data which the service provider transmits or stores; or
- (b) actively seek facts or circumstances indicating an unlawful activity.

[...]

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

*Effect of non-liability provisions*

If, in relation to particular illicit content or activity, an online intermediary satisfies all of the applicable conditions for availing itself to the protection of a safe harbour, then that online intermediary will be protected from civil and/or criminal liability (as the case may be, under the law in question) in relation to such illicit content or activity. Some non-liability regimes, such as that contained in the South African Electronic Communications and Transactions Act, 2002, set out below, also expressly protect online intermediaries from civil liability for the removal of content pursuant to the provision. The Computer Misuse and Cybercrimes Act, 2018 of Kenya contains a further protection from liability for the disclosure of data or other information required by the Act.

**EXAMPLE: SOUTH AFRICA – ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002****Take-down notification**

77. [...]

(3) A service provider is not liable for wrongful take-down in response to a notification.

**EXAMPLE: KENYA – COMPUTER MISUSE AND CYBERCRIMES ACT, 2018****Confidentiality and limitation of liability**

56. [...]

(3) A service provider shall not be liable under this Act or any other law for the disclosure of any data or other information that the service provider discloses only to the extent required under this Act or in compliance with the exercise of powers under this Part.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*



Finally, it is important to note that the fact that an online intermediary cannot avail itself of the protections of a safe harbour does not mean that the online intermediary has committed any offence or civil wrong. For the online intermediary to be liable in relation to the illicit content or activity, an offence or cause of action against the online intermediary must still be established. That being said, some of the matters which are relevant to disqualifying an online intermediary from the protection of a safe harbour, such as knowledge of the illicit content or activity, may also be relevant to establishing its liability, if a case is brought against the intermediary.<sup>165</sup>

## ISSUES COMMON TO COOPERATION- AND LIABILITY-BASED APPROACHES

This chapter's discussion of policy issues has thus far been divided into issues concerning cooperation-based approaches and liability-based approaches. There are, however, several further issues that policymakers and legislators will need to consider that are common to both types of approaches. These issues may include legal issues, such as issues relating to jurisdiction, and practical issues, such as challenges of removing content and services on the basis of terms of service and the need for transparency and appropriate procedures for monitoring, evaluating and adapting measures.

### Jurisdiction

Jurisdiction concerns “the power of the state under international law to regulate or otherwise impact upon people, property and circumstances”.<sup>166</sup> Issues of jurisdiction are at the heart of Internet governance<sup>167</sup> and policy approaches to prevent and combat wildlife crime, falsified medical products-related crime and trafficking in cultural property online are no exception. These include issues relating to the laws applicable to online intermediaries that are based in multiple jurisdictions or which provide services across borders and cross-border access to electronic evidence by law enforcement.

Under international law, including the Organized Crime Convention, the principal ground for the exercise of criminal jurisdiction is territorial (the territorial principle).<sup>168</sup> The territorial principle applies so long as at least part of an offence occurs within the territory of the State.<sup>169</sup> States may also exercise jurisdiction in relation to, inter alia, crimes committed by their nationals (the active personality principle), crimes committed against its nationals (the passive personality principle) and crimes which affect the State's essential interests (the protective principle).<sup>170</sup> The result is that, in relation to wildlife crime, falsified medical products-related crime and trafficking in cultural property committed online, there may be a large number of countries that can exercise jurisdiction in respect of a particular case. Consider the application of only the territorial principle in respect of such conduct:

At least four territorial factors can play a role in determining applicable law: the location(s) of internet end-user(s) or connected devices; the location(s) of the servers or devices that store or process the actual data; the locus of incorporation of the internet companies that run the service(s) in question; and, in the case of the world wide web, the registrars or registries through which a domain name is registered.<sup>171</sup>

When other principles of jurisdiction are applied, the number of countries that may exercise jurisdiction in relation to particular offences is even greater. Several of the key issues relating to jurisdiction online arise as

<sup>165</sup> Park, “From liability trap to the world's safest harbour”, pp. 251 and 260.

<sup>166</sup> Malcolm N. Shaw, *International Law*, 8th ed. (Cambridge, United Kingdom, Cambridge University Press, 2017), p. 483.

<sup>167</sup> Bertrand de la Chapelle and Paul Fehlinger, “Jurisdiction on the Internet: from legal arms race to transnational cooperation”, in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 727 and 730.

<sup>168</sup> Shaw, *International Law*, p. 489.

<sup>169</sup> Ibid., p. 490.

<sup>170</sup> Ibid., pp. 496–497 and 499.

<sup>171</sup> Chapelle and Fehlinger, “Jurisdiction on the Internet”, pp. 727 and 729.

a result of online intermediaries being simultaneously subject to the laws of multiple jurisdictions in respect of the same conduct. As noted by one commentator:

while most people would expect internet intermediaries to abide by the law of their respective countries, they would probably not wish for internet intermediaries to abide by all laws of all other countries in the world. In the end, such compliance would lead to internet intermediaries being forced to take account only of the most restrictive laws from all the countries in the world.<sup>172</sup>

In some countries, online intermediaries operating in multiple jurisdictions have nevertheless been ordered to block or remove content hosted in or accessible in other jurisdictions. In *LICRA v. Yahoo! Inc.*, for example, a French court ordered the United States-based parent company of Yahoo France, Yahoo! Inc, to prohibit French users from accessing postings displaying Nazi memorabilia on the parent company's website.<sup>173</sup> In *Equustek Solutions Inc v. Google Inc.*, the Court of Appeal for British Columbia upheld the decision of the Supreme Court of British Columbia to grant an injunction requiring Google to remove search results pointing to a particular website globally.<sup>174</sup> In *British Columbia (Attorney General) v. Brecknell*, the Court of Appeal of British Columbia, drawing on its earlier decision in *Equustek*, held that Craigslist, a website for classified advertisements, could be compelled by a British Columbia court to produce documents located outside Canada, notwithstanding that Craigslist had no physical presence in British Columbia.<sup>175</sup>

In some cases, the multiple laws to which online intermediaries are subject may be in conflict with each other. For example, where an online intermediary is served with a warrant for the search and seizure of data located on servers in another jurisdiction, the online intermediary may be placed in a position where compliance with the search warrant may be in breach of data protection or other laws of the country in which the servers are located.<sup>176</sup>

Further jurisdictional issues relate to cross-border access to electronic evidence by law enforcement. The use of online services by criminals engaged in wildlife crime, falsified medical products-related crime or trafficking in cultural property poses numerous challenges for law enforcement. Electronic evidence of unlawful activity may often be located on servers outside of the territory of the investigating agency. Law enforcement agencies may need to access basic subscriber information, traffic data and/or content data abroad. They may also need to intercept traffic and/or content data in real-time. Depending on the nature of the request, electronic evidence may be requested from online intermediaries directly, through police-to-police cooperation, or through mutual legal assistance (MLA) requests. It is important that any such procedures be designed in ways that ensure that procedural safeguards, adequate oversight and access to remedies are not weakened or circumvented.<sup>177</sup>

The Internet poses both practical and legal challenges in this regard. Where data is hosted on the Cloud, parts of the data may be located in different States. This poses challenges for law enforcement in knowing where requests for electronic evidence should be directed. Legal issues include those surrounding when a State has jurisdiction to require the production of electronic evidence abroad and the possibility of conflict with foreign legislation, such as data protection laws.

<sup>172</sup> Dan Jerker B. Svantesson, "Internet jurisdiction and intermediary liability", in *The Oxford Handbook of Online Intermediary Liability*, Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 691 and 693.

<sup>173</sup> TGI de Paris, ordonnance de référé du 20 novembre 2000. See further *UEJF and Licra v. Yahoo! Inc and Yahoo France*.

<sup>174</sup> *Equustek Solutions Inc v. Google Inc.*, 2015 BCCA 265. See further Michael Geist, "The *Equustek* effect: a Canadian perspective on global takedown orders in the age of the Internet", *The Oxford Handbook of Online Intermediary Liability*, in Giancarlo Frosio, ed. (Oxford, Oxford University Press, 2020), pp. 709, 712–714.

<sup>175</sup> *British Columbia (Attorney General) v. Brecknell*, 2018 BCCA 5. See further Geist, "The *Equustek* effect", pp. 709, 722–723.

<sup>176</sup> See further Svantesson, "Internet jurisdiction and intermediary liability", pp. 691, 697–698.

<sup>177</sup> A/HRC/39/29, para. 22.

## Terms of service-based removal of content and withdrawal of services

A further issue relating to both cooperation- and liability-based approaches concerns the removal of content and the withdrawal of services by online intermediaries on the basis of their terms of service. In chapter 2, it was explained that the relations between online intermediaries and their users are governed both by the applicable law and contracts known as terms of service. When an online intermediary takes action to remove content or withdraw access to a service, the online intermediary may do so on the basis that the content or activity in question breaches either the law or on the basis of their terms of service. In practice, it is often easier for online intermediaries to do so on the basis of the latter. This is because the grounds for removal of content or withdrawal of a service that an online intermediary may exercise under its terms of service are generally broader than the grounds for which such content or service must be removed or withdrawn under the applicable law. Online intermediaries will also often be more familiar with their own terms of service than the applicable law, particularly when they operate in multiple jurisdictions and are hence subject to the laws of each of these jurisdictions.

When online intermediaries remove content or withdraw services on the basis of their terms of service, the content or activity may not be identified by the online intermediary as being illegal. This may mean that content is not brought to the attention of and hence investigated by law enforcement authorities. This may also lead to poorer data about the scale of crime online if, for example, cases of trafficking in wildlife products, falsified medical products or cultural property are reported by online intermediaries in transparency reports as mere terms-of-service violations.

This issue can be addressed, in part, by States ensuring that users of the services of online intermediaries have accessible means of directly reporting suspected unlawful content or activity to law enforcement authorities. This issue may also be addressed by encouraging or requiring online intermediaries to make assessments as to the unlawfulness of certain content or activities, to report suspected cases of certain serious crimes to law enforcement authorities for further investigation and to preserve any relevant data. Several examples of legislative provisions requiring online intermediaries to take such steps were set out earlier in this chapter. Where it is mandatory for online intermediaries to make such reports to law enforcement authorities, States should ensure that both the circumstances in which reports must be made and the content of such reports are proportionate to the policy goals in question to ensure, *inter alia*, respect for users' privacy.

In Germany, § 3 of the NetzDG, an excerpt of which is set out on page 41, requires, *inter alia*, that social media providers to which the law applies that are in receipt of a complaint about unlawful content examine whether the content to which the complaint relates is unlawful and remove or block access to unlawful content.<sup>178</sup> An amendment to NetzDG, which will enter into force on 1 February 2022, will further require social media providers to which the law applies that receive reports of certain forms of unlawful content to report such content to the German Federal Criminal Police Office.<sup>179</sup>

<sup>178</sup> Germany, Network Enforcement Act (NetzDG), sect. 3, para. 2.

<sup>179</sup> *Ibid.*, sect. 3a, *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität*. (Law on Combating Right-Wing Extremism and Hate Crimes).

### EXAMPLE: GERMANY –NETWORK ENFORCEMENT LAW (NETZWERKDURCHSETZUNGSGESETZ)<sup>a</sup>

#### Section 3a

##### Notification obligation

(1) The provider of a social network must maintain an effective procedure for reporting in accordance with paragraphs 2 to 5.

(2) The provider of a social network must transmit content to the Federal Criminal Police Office as a central body for the purpose of enabling the prosecution of criminal offences,

1. that have been reported to the provider in a complaint about illegal content,
2. which the provider removes or to which he has blocked access and
3. where there is concrete evidence that they are at least one of the facts
  - a) §§ 86, 86a, 89a, 91, 126, 129 to 129b, 130, 131 or 140 of the Criminal Code,
  - b) of § 184b in conjunction with § 184d of the Criminal Code or
  - c) § 241 of the Criminal Code in the form of a threat to a crime against life, sexual self-determination, physical integrity or personal freedom are fulfilled and are not justified.

(3) The provider of the social network must immediately after removing or blocking access to the content, check whether the requirements of paragraph 2(3) are met and immediately transmit the content in accordance with paragraph 4.

(4) The transmission to the Federal Criminal Police Office must include:

1. the content and, if available, the time at which the content was shared or made available to the public, indicating the underlying time zone,
2. the following information about the user who shared the content with other users or made it available to the public:
  - a) the user name and,
  - b) if available, the last IP address used in relation to the social network provider, including the port number and the time of the last access, indicating the underlying time zone.

(5) The transmission to the Federal Criminal Police Office must be carried out electronically via an interface provided by the Federal Criminal Police Office.

(6) The provider of the social network informs the user for whom the content was saved 4 weeks after the transmission to the Federal Criminal Police Office about the transmission in accordance with paragraph 4. Sentence 1 does not apply if the Federal Criminal Police Office orders within 4 weeks that the information must be deferred because of the threat to the purpose of the investigation, life, physical integrity or personal freedom of a person or significant assets. In the case of an order according to sentence 2, the Federal Criminal Police Office will inform the user of the transmission according to paragraph 4 as soon as this is possible without any danger according to sentence 2.

(7) The provider of a social network has to provide the administrative authority named in § 4 with information on their request on how the procedures for the transmission of content according to paragraph 1 are designed and how they are used.

(8) Law enforcement authorities may, for the purposes of a general discussion with social networking providers on the application of paragraphs 1 to 7, process the personal data necessary for that purpose in a pseudonymised form.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

<sup>a</sup> English translation provided by the German Federal Ministry of Justice and Consumer Protection.

## Monitoring, evaluating and adapting measures and the need for transparency

Effective policymaking is contingent upon learning from experience. Whatever measures are taken to address wildlife crime, falsified medical products-related crime and trafficking in cultural property online – whether cooperation- or liability-based – it is critical that States monitor, evaluate and adapt such measures to ensure their effectiveness and proportionality. To do so, it is important that policymakers, and the public, have access to meaningful data. This requires a certain measure of transparency, both from States themselves and from online intermediaries.<sup>180</sup> Transparency, monitoring, evaluation and adaptation are important both to ensure the effectiveness of policy measures in achieving their intended purposes and to protect the exercise of human rights such as freedom of expression, the right to peaceful assembly and the right to privacy online.<sup>181</sup>

Meaningful data upon which policy measures can be evaluated should include the data relating to the scope, nature and evolution of wildlife crime, falsified medical products-related crime and trafficking in cultural property online. It should also include data measuring the impact of measures taken by States and industry on these crimes as well as the impact of these measures on legitimate content and activity online. Transparency reports of online intermediaries are an important tool for analysis in this regard. To provide meaningful data for analysis, transparency reports must, at a minimum, distinguish between actions taken by the online intermediary on the basis that the content or activity is unlawful and actions taken on the basis that the content or activity is merely in breach of the online intermediary's terms of service. At present, it is rare for online intermediaries to distinguish between such actions in their transparency reports. The data published in transparency reports should also be consistent over time to allow trends to be analysed. Likewise, it is beneficial if different online intermediaries use standardized methodologies of reporting data to allow cross-platform analysis.

Some legislative schemes contain provisions that seek to improve the transparency of actions taken by online intermediaries in relation to unlawful content or activity. For example, § 2 of the German NetzDG, set out below, requires that social media providers which operate for profit, have more than two million registered users in Germany, and receive more than 100 complaints about unlawful content per calendar year, must produce half-yearly reports on the handling of such complaints on their platforms.<sup>182</sup> Such reports must include, inter alia, the total number of complaints received in the reporting period and the number of complaints that resulted in the deletion or blocking of the content in question, broken down according to whether the complaints were submitted by complaints bodies or by users and according to the reason for the complaint as well as the time between the receipt of complaints and the unlawful content being deleted or blocked.<sup>183</sup>

### EXAMPLE: GERMANY – NETWORK ENFORCEMENT LAW (NETZWERKDURCHSETZUNGSGESETZ )<sup>a</sup>

#### Section 2

#### Reporting obligation

(1) Providers of social networks which receive more than 100 complaints per calendar year about unlawful content shall be obliged to produce half-yearly German-language reports on the handling of complaints about unlawful content on their platforms, covering the points enumerated in subsection (2), and shall be obliged to

<sup>180</sup> A/HRC/38/35, paras. 52, 64, 69, 71–72.

<sup>181</sup> Human rights dimensions of policy measures in this area are further discussed in chapter 5.

<sup>182</sup> Germany, Network Enforcement Act (NetzDG), sect. 2, para. 1.

<sup>183</sup> Ibid., sect. 2, para. 2.



publish these reports in the Federal Gazette and on their own website no later than one month after the half-year concerned has ended. The reports published on their own website shall be easily recognisable, directly accessible and permanently available.

(2) The reports shall cover at least the following points:

1. general observations outlining the efforts undertaken by the provider of the social network to eliminate criminally punishable activity on the platform,
2. description of the mechanisms for submitting complaints about unlawful content and the criteria applied in deciding whether to delete or block unlawful content,
3. number of incoming complaints about unlawful content in the reporting period, broken down according to whether the complaints were submitted by complaints bodies or by users, and according to the reason for the complaint,
4. organisation, personnel resources, specialist and linguistic expertise in the units responsible for processing complaints, as well as training and support of the persons responsible for processing complaints,
5. membership of industry associations with an indication as to whether these industry associations have a complaints service,
6. number of complaints for which an external body was consulted in preparation for making the decision,
7. number of complaints in the reporting period that resulted in the deletion or blocking of the content at issue, broken down according to whether the complaints were submitted by complaints bodies or by users, according to the reason for the complaint, according to whether the case fell under section 3 subsection (2) number (3) letter (a), and if so, whether the complaint was forwarded to the user, and whether the matter was referred to a recognised self-regulation institution pursuant to section 3 subsection (2) number (3) letter (b),
8. time between complaints being received by the social network and the unlawful content being deleted or blocked, broken down according to whether the complaints were submitted by complaints bodies or by users, according to the reason for the complaint, and into the periods “within 24 hours”/“within 48 hours”/“within a week”/“at some later point”,
9. measures to inform the person who submitted the complaint, and the user for whom the content at issue was saved, about the decision on the complaint.

*Disclaimer: the inclusion of legislative examples in this issue paper is for illustrative purposes only and does not constitute an endorsement of a provision, approach or legislative scheme*

<sup>a</sup>English translation provided by the German Federal Ministry of Justice and Consumer Protection.

Monitoring and evaluation of measures must take place on an ongoing basis. Criminals engaged in wildlife crime, falsified medical products-related crime or trafficking in cultural property online adapt their behaviour in response to policy measures taken by States and actions taken by online intermediaries in an effort to avoid detection. Additionally, the interests of and incentives for online intermediaries also change over time. Developments in the nature of these crimes and in industry must be duly monitored to identify policy deficiencies and possibilities for improvement. When deficiencies and possibilities for improvement are identified, States must adapt their policies to effectively prevent and combat the commission of these crimes online.

The Europol *SIRIUS EU Digital Evidence Situation Report 2019* is a noteworthy example of good data collection and analysis.<sup>184</sup> The report describes the current status of access of European Union member States to electronic evidence held by online intermediaries based in foreign jurisdictions. The report is based on information from online intermediaries' publicly available transparency reports, online surveys with European Union law enforcement and judicial authorities, and interviews with online service providers. The report explains challenges faced by both law enforcement authorities and online intermediaries and provides an analysis of the roots of these problems. The report provides an example of the type of detailed analysis that is necessary to design and update policies in a rapidly evolving digital space.

## CONCLUSION

This chapter has considered several broad categories of non-mutually exclusive policy measures for addressing wildlife crime, falsified medical products-related crime and trafficking in cultural property online and the key considerations and issues relating to each type. Cooperation-based measures involve policymakers seeking to have industry cooperate with law enforcement authorities to prevent and combat illicit activity online. Cooperation-based measures may be based on self-regulatory or co-regulatory approaches. The success of such approaches depends upon a number of factors, including the capacity of industry participants to prevent and combat the illicit activity in question, the extent to which industry interests align with public policy goals, the strength of the commitments made by participants, the extent to which the scheme covers the industry in question, the extent to which participants adhere to their commitments and the consequences of not doing so.

Liability-based measures seek to prevent and combat illicit activity online through defining or circumscribing circumstances in which intermediaries may be held liable in relation to illicit activities occurring over their services. Liability-based measures may involve both provisions which establish liability and which protect from liability. Since the mid-1990s, legislative activity governing the conditions under which online intermediaries may be liable for wrongful conduct has been dominated by the introduction of non-liability provisions.

Rules establishing liability for online intermediaries relevant to wildlife crime, falsified medical products-related crime and trafficking in cultural property online can be broadly categorized into secondary and inchoate liability for primary offences, on the one hand, and rules establishing offences for breach of statutory duties on the other. Rules of secondary and inchoate liability tend not to be specifically targeted at online intermediaries and are rather generally applicable to all natural and legal persons. Secondary liability and offences of conspiracy tend to require proof of higher degrees of fault on the part of the offender and hence generally require proof of knowledge or intention. An online intermediary could be guilty of aiding or abetting the commission of one of these crimes where they provide a service to a user, intending or knowing that that user would use the service to commit such an offence. An online intermediary could likewise be guilty of counselling, procuring or facilitating the commission of an offence if they could be proven to have designed or marketed a product with this intent. Offences of conspiracy may be relevant where an online intermediary enters into an agreement with one or more other persons to provide services for the purposes of committing offences relating to wildlife crime, falsified medical products-related crime or trafficking in cultural property. As the vast majority of online intermediaries have no specific intention of facilitating illegal activity, such offences will be of limited relevance to them in practice.

More relevant to online intermediaries are offences for breach of statutory duties. There are a broad range of such offences, including duties to remove or disable access to content, to retain data, to report knowledge of unlawful content to relevant authorities, to disclose information requested by or otherwise render assistance to a law enforcement agency, or to refrain from disclosing that an order (such as a preservation or production order) was made and that any action was taken or data collected under the order.

<sup>184</sup> Europol, "SIRIUS EU digital evidence situation report 2019: cross-border access to electronic evidence" (The Hague, 2019).

Non-liability regimes may also vary between countries, according to whether they are horizontal or vertical, whether they provide immunity from civil or criminal liability or both, the conditions for availing of safe harbour, whether they expressly establish notice and takedown regimes and the nature of such regimes, whether they include Good Samaritan or non-monitoring provisions, and the effect of protection within the safe harbour. The conditions which an online intermediary must meet in order to avail itself of the safe harbour commonly include conditions relating to the functions exercised by the online intermediary, its knowledge of the illicit content or activity, and its conduct upon obtaining knowledge of illicit content or activities.

Jurisdictional issues, including challenges posed by online intermediaries being subjected to laws from multiple jurisdictions, the potential for conflict between these laws, and practical challenges for law enforcement access to electronic evidence across borders, are common to both cooperation- and liability-based approaches.

This chapter has shown that the toolkit of policymakers in addressing wildlife crime, falsified medical products-related crime and trafficking in cultural property online is varied and complex. The measures set out in this chapter – cooperation- and liability-based measures, including both liability and non-liability rules – are not and should not be considered mutually exclusive. In developing an approach to prevent and combat these crimes, States should consider all appropriate policy options. Policy approaches should seek to provide online intermediaries with the right balance of incentives – to effectively support the State's efforts to prevent and combat these crimes in a manner which is proportionate, which does not infringe upon the exercise of users' rights, and which allows legitimate online activities to flourish.

Achieving this balance is difficult. Policy measures which seek to address one problem can cause others. Whereas non-liability provisions seek, *inter alia*, to provide online intermediaries with sufficient legal certainty to provide socially important online services, conditioning access to safe harbours on online intermediaries being passive, rather than active, or not having knowledge of illicit content or activity can incentivize online intermediaries to do as little as possible to manage user content. Good Samaritan provisions seek to address this problem but without effective safeguards can encourage excessive removal of content by online intermediaries. Notice and takedown regimes seek to facilitate the removal of illicit content by providing mechanisms for users of online services to alert online intermediaries as to content that appears to be in breach of the law. However, when online intermediaries' access to safe harbours is premised on expeditiously removing unlawful content in response to user notices, online intermediaries may be required to make assessments as to the legality of content that they are not well-positioned to make. When online intermediaries are faced with uncertainty as to whether failure to remove content may result in loss of protection from liability, they will naturally be incentivized to err on the side of caution in avoiding liability. Trusted notifiers are a mechanism that has been proposed to address the issue of online intermediaries lacking the necessary resources and expertise to assess the legality of content, but overreliance of online intermediaries on trusted notifiers, "rubber-stamping" their assessments, entails further risks of lawful content being removed. These are just some examples of the challenges faced by policymakers in seeking to address wildlife crime, falsified medical products-related crime and trafficking in cultural property online.

This chapter provides no concrete answers on how to effectively achieve the appropriate balance of incentives for online intermediaries but has rather sought to identify key considerations and issues concerning some of the main types of policy measures for preventing and combating the online commission of the three types of crime covered by this paper.

Whatever the approach taken by policymakers, the success and sustainability of this approach will depend on the extent to which States monitor, evaluate and adapt their measures to ensure their effectiveness and proportionality. Effective policymaking is contingent upon learning from experience. This requires a certain measure of transparency, both from States themselves and from online intermediaries.





---

# Chapter 5.

## HUMAN RIGHTS

Chapter 1 of this issue paper outlined the seriousness of wildlife crime, falsified medical products-related crime and trafficking in cultural property. These crimes cause serious harm to human health, human security, societies, economies, cultures, animals and the environment. In so doing, they threaten the exercise of a number of human rights. The seriousness of these crimes demands that States take action to prevent and combat them, including when they are committed online.

At the same time, policy measures taken by States to address crime online also have the potential to significantly undermine the exercise of human rights. The digitization of society has both created huge opportunities for the exercise of human rights and rendered the free exercise of human rights increasingly reliant on the digital sphere. Today, we use the Internet to exercise many human rights, including freedom of expression and freedom of assembly. The power of the Internet to allow anyone to communicate with anyone, without permission and with low barriers to doing so is at the core of its success, both economically and socially. At the same time, the digitization of society has led to the processing of growing volumes of personal data, with far-reaching implications for the exercise of rights such as the right to privacy.

Actions (or the inaction) of States in governing online spaces can affect the exercise of each of these rights. Policy measures taken by States may impact the exercise of human rights directly, or they may affect the exercise of human rights indirectly through the actions they cause online intermediaries to take. For example, when States expose online intermediaries to liability, the steps taken by intermediaries to comply with the law may result in restrictions on the free exercise of human rights by their users. Where an online intermediary chooses to more aggressively remove the content it hosts to protect itself from liability, this may result in negative effects on the exercise of the right to freedom of expression of many users. The exercise of human rights may also be affected by other actions taken by online intermediaries to minimize their exposure to liability, such as monitoring, filtering and restricting content. For example, policies that ban all content suspected of involving wildlife trafficking may also prevent wildlife activists from discussing conservation or sharing photos of wildlife crime to raise awareness, or animal shelters from posting adoption advertisements.

In this context, it is also important to note that while States have legal tools available to them to encourage or coerce online intermediaries to take actions in pursuit of particular policy goals – and while States also dispose of certain tools to prevent or mitigate negative impacts on human rights, such as transparency measures and access to remedies – it is more difficult for States to prevent private intermediaries from making particular

choices to protect themselves from liability when these choices result in excessive restrictions on users such as through the withdrawal of services or the filtering or blocking of activities online.

Each of the aforementioned factors necessitates careful and nuanced policymaking which balances the legitimate aims of policy interventions against the potential collateral and counterproductive effects of these interventions, including on the exercise of human rights. It is critical that States adequately assess and take into consideration the human rights implications of policy interventions. This is the case whether the potential effects on the exercise of human rights are the direct result of a policy intervention or the result of the actions taken by intermediaries and others in response to State policy. States have a duty under international human rights law to respect, protect and fulfil the human rights of persons within their territory and under their jurisdiction. According to the *Guiding Principles on Business and Human Rights*, adopted by the Human Rights Council, this includes a duty to protect against infringements of human rights by third parties, including businesses.<sup>185</sup> The Committee on Economic, Social and Cultural Rights has stated that States must adopt “legislative, administrative, educational and other appropriate measures” to ensure effective protection against human rights violations by businesses,<sup>186</sup> and has noted that “State parties should consider imposing criminal or administrative sanctions and penalties, as appropriate, where business activities result in abuses of Covenant rights or where a failure to act with due diligence to mitigate risks allows such infringements to occur”.<sup>187</sup>

This chapter seeks to provide policymakers with an outline of the key considerations relating to human rights that must be considered when designing policy measures to address wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online. It begins with a short overview of the rights implicated by each of the three types of crime considered by this paper. It then considers how the policy measures discussed in this paper may affect the exercise of human rights. Following this, it discusses the circumstances in which States can lawfully restrict the exercise of human rights, in the context of the policy measures and goals discussed in the paper. Finally, it makes reference to further resources for building human rights-based approaches.

The discussion in this chapter is based primarily on the International Covenant for Civil and Political Rights (ICCPR) and the International Covenant for Economic, Social and Cultural Rights (ICESCR) as the leading international human rights instruments. States also have obligations under other international and regional human rights instruments, such as the Convention on the Rights of the Child, the African Charter on Human and Peoples’ Rights, the American Convention on Human Rights and the European Convention on Human Rights, as well as customary international law.<sup>188</sup> Where relevant, this chapter also makes reference to rights contained in these international and regional instruments. Finally, it should be noted that States may also have human rights obligations under national constitutions and bills of rights.

This chapter discusses the rights implicated by wildlife crime, falsified medical products-related crime and trafficking in cultural property prior to the rights implicated by policy responses to the commission of these crimes online because the crimes are logically anterior to the response thereto. Neither the structure nor content of this chapter should be understood to emphasize the importance of any rights over others. Indeed, both the International Covenant on Civil and Political Rights and International Covenant on Economic, Social and Cultural Rights expressly state that there shall be no restriction upon or derogation from any of the fundamental rights recognized or existing in any country pursuant to law, conventions, regulations or customs on the pretext that the Covenant does not recognize such rights or that it recognizes them to a lesser extent.<sup>189</sup>

<sup>185</sup> Human Rights Council resolution 17/4, para. 1.

<sup>186</sup> Committee on Economic, Social and Cultural Rights, general comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, para. 14.

<sup>187</sup> *Ibid.*, para. 15.

<sup>188</sup> See further, Richard B. Lillich, “The growing importance of customary international human rights law”, *Georgia Journal of International and Comparative Law*, vol. 25, No. 1 (1996).

<sup>189</sup> International Covenant on Civil and Political Rights, art. 5(2); International Covenant on Economic, Social and Cultural Rights, art. 5(2).



## RIGHTS IMPLICATED BY WILDLIFE CRIME, FALSIFIED MEDICAL PRODUCTS-RELATED CRIME AND TRAFFICKING IN CULTURAL PROPERTY

As noted above, wildlife crime, falsified medical products-related crime and trafficking in cultural property are serious crimes which cause serious harm. They also threaten the exercise of a number of human rights. Whereas chapter 1 considered the harm caused by these crimes, this section considers the human rights obligations of States in relation to these crimes in light of the serious harm that they cause. It seeks to provide a brief overview of some of several key rights implicated by each of these crimes: the right to health, the right to life and the right to take part in cultural life. This section should not be considered an exhaustive statement of the rights implicated by these crimes. Indeed, as human rights are interlinked, the crimes discussed in this paper may affect the exercise and realization of a number of human rights.

### Rights to health and to life

The manufacture and trafficking of falsified medical products can threaten the exercise of the right to health and, in some cases, the right to life. As was noted in chapter 1, falsified medical products may be of poor quality, unsafe or ineffective, endangering health, prolonging illness, promoting antimicrobial resistance and the spread of drug-resistant infection, or potentially killing patients. The right to health is recognized in the International Covenant on Economic, Social and Cultural Rights as well as numerous other international and regional human rights instruments.<sup>190</sup> Health is a “fundamental human right indispensable for the exercise of other human rights”.<sup>191</sup> The Committee on Economic, Social and Cultural Rights has noted that the right to health “must be understood as a right to the enjoyment of a variety of facilities, goods, services and conditions necessary for the realization of the highest attainable standard of health”.<sup>192</sup> Availability, accessibility, acceptability and – importantly in this context – quality of health facilities, goods and services are essential and interrelated elements of the right to health.<sup>193</sup> As with other human rights, the right to health entails obligations to respect, protect and fulfil the right.<sup>194</sup> The obligation to protect requires States to take measures that prevent third parties from interfering with the right to health.<sup>195</sup> Accordingly, the right to health could be understood as entailing some level of obligation to prevent and combat the manufacture and trafficking of falsified medical products that threaten the health of persons within the territory or subject to the jurisdiction of the State.

The right to health also entails an obligation for States to take steps necessary for the “prevention, treatment and control of epidemic, endemic, occupational and other diseases”<sup>196</sup> and “the improvement of all aspects of environmental and industrial hygiene”;<sup>197</sup> the latter comprising, inter alia, “the prevention and reduction of the populations exposure to ... detrimental environmental conditions that directly or indirectly impact upon human health”.<sup>198</sup> Insofar as wildlife trafficking contributes to the spread of zoonotic diseases and environmental degradation, States should take preventive steps against such trafficking.

<sup>190</sup> See International Covenant on Economic, Social and Cultural Rights, art. 12; Convention on the Rights of the Child, art. 24; African Charter on Human and Peoples’ Rights, art. 16; Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights (Protocol of San Salvador), art. 10. For a list of further instruments, see Committee on Economic, Social and Cultural Rights, general comment No. 14 (2000) on the right to the highest attainable standard of health, para. 2.

<sup>191</sup> General comment No. 14 (2000), para. 1.

<sup>192</sup> Ibid., para. 9.

<sup>193</sup> Ibid., para. 12.

<sup>194</sup> Ibid., para. 33.

<sup>195</sup> Ibid. See also Committee on Economic, Social and Cultural Rights, general comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, para. 18.

<sup>196</sup> International Covenant on Economic, Social and Cultural Rights, art. 12, para. 2 (c).

<sup>197</sup> Ibid., art. 12, para. 2 (b).

<sup>198</sup> Committee on Economic, Social and Cultural Rights, general comment No. 14 (2000), para. 15.

Falsified medical products and wildlife crime – through its contribution to the spread of zoonotic diseases – may also threaten the exercise of the right to life. The right to life is a fundamental right,<sup>199</sup> “the effective protection of which is the prerequisite for the enjoyment of all other human rights and the content of which can be informed by other human rights”.<sup>200</sup> The right to life entails an obligation for States “to adopt any appropriate laws or other measures in order to protect life from all reasonably foreseeable threats, including from threats emanating from private persons and entities”.<sup>201</sup> As further outlined in chapter 1, falsified medical products pose such threats. To the extent that wildlife trafficking contributes to the spread of zoonotic diseases and environmental degradation, it too poses a reasonably foreseeable threat to the right to life against which States should protect individuals within their territory and subject to their jurisdiction.<sup>202</sup>

## Right to take part in cultural life

The right to take part in cultural life,<sup>203</sup> like other human rights, entails obligations of States to respect, protect and to fulfil.<sup>204</sup> The protection of cultural diversity is inseparable from respect for human dignity.<sup>205</sup> The obligation to protect requires States to prevent third parties from interfering in the right to take part in cultural life.<sup>206</sup> States must protect cultural heritage in all its forms, in times of war and peace, and natural disasters.<sup>207</sup> States must protect and preserve “historical sites, monuments, works of art and literary works”,<sup>208</sup> among other cultural goods.<sup>209</sup> As noted in chapter 1, trafficking in cultural property is a crime that harms cultural heritage and can undermine cultural rights, including the right to take part in cultural life.<sup>210</sup> States should therefore take steps to prevent and combat trafficking in cultural property.

## RIGHTS IMPLICATED BY POLICY MEASURES ADDRESSING WILDLIFE CRIME, FALSIFIED MEDICAL PRODUCTS-RELATED CRIME AND TRAFFICKING IN CULTURAL PROPERTY ONLINE

The human rights affected by wildlife crime, falsified medical products-related crime and trafficking in cultural property are not the only human rights that States must consider in addressing these crimes when they occur online. It is equally incumbent upon States to consider the human rights implications of the policy measures they adopt to address these crimes. It is worth repeating that this includes the direct consequences of policy measures on the exercise of human rights and the consequences of actions taken by intermediaries and others in response to State policy.

<sup>199</sup> See International Covenant on Civil and Political Rights, art. 6; Convention on the Rights of the Child, art. 6; African Charter on Human and Peoples’ Rights, art. 4; American Convention on Human Rights, art. 4; European Convention on Human Rights, art. 2.

<sup>200</sup> Human Rights Committee, general comment No. 36 (2019), para. 2.

<sup>201</sup> Ibid., paras. 18–22.

<sup>202</sup> See also Human Rights Committee, general comment No. 36 (2019) on the right to life, paras. 26 and 62, which expressly mention “the prevalence of life-threatening diseases” and “environmental degradation” as threats to the right to life against which States must take action to protect.

<sup>203</sup> International Covenant on Economic, Social and Cultural Rights, art. 15, para. 1 (a); Convention on the Rights of the Child, art. 31; African Charter on Human and Peoples’ Rights, art. 17, para. 2; Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights (Protocol of San Salvador), art. 14, para. 1 (a).

<sup>204</sup> Committee on Economic, Social and Cultural Rights, general comment No. 21 (2009) on the right of everyone to take part in cultural life, para. 48.

<sup>205</sup> Ibid., para. 40.

<sup>206</sup> Ibid., para. 48.

<sup>207</sup> Ibid., para. 50.

<sup>208</sup> Ibid.

<sup>209</sup> Ibid., para. 43.

<sup>210</sup> As affirmed in Human Rights Council resolution 37/17 on cultural rights and the protection of cultural heritage, and recalled in General Assembly resolution 73/13 on the return or restitution of cultural property to the countries of origin.

This section seeks to provide a brief overview of some of the key rights which may be affected by the policy measures discussed in this paper: freedom of expression, the right of peaceful assembly, the right to privacy and the right to remedy. As with the previous section, this section should not be considered an exhaustive statement of the rights potentially affected by policy measures in this area.

## Freedom of expression

Freedom of expression includes “freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice”.<sup>211</sup> Freedom of expression,<sup>212</sup> together with freedom of opinion, are “indispensable conditions for the full development of the person” and “constitute the foundation stone for every free and democratic society”.<sup>213</sup> Freedom of expression is “a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights”.<sup>214</sup> Like other human rights, it entails obligations to respect, protect and fulfil. The Human Rights Committee has stated that the obligation to protect “requires States parties to ensure that persons are protected from any acts by private persons or entities that would impair the enjoyment of the freedoms of opinion and expression to the extent that these Covenant rights are amenable to application between private persons or entities”.<sup>215</sup>

The functionality of the Internet, which allows anyone to communicate with anyone, without permission and with low barriers to doing so, brings with it significant opportunities for the realization of freedom of expression. Websites, blogs, messaging services and other technologies offer previously unimaginable possibilities for people to communicate freely with each other. The importance of the Internet for communicating and connecting with each other has been clearly highlighted by the COVID-19 crisis as education, physical and mental health services, social life, family relations, commerce and political organization moved online to prevent the further spread of the disease.

Actions such as surveillance, filtering, blocking and removal of communications – whether required by legislation or undertaken voluntarily by online intermediaries – have implications for the exercise of freedom of expression. This is especially the case as a number of online industries such as social media become increasingly dominated by a handful of intermediaries, with the result that few or no meaningful alternatives exist when access to the service is restricted for a particular user. Any law that requires an online intermediary to unduly limit freedom of expression risks violating the obligation to respect this right. A law which fails to protect persons from actions of online intermediaries that unduly limit freedom of expression may constitute a violation of the obligation to protect. Once again, it is important to note the risk that policy measures create incentives for intermediaries to “overcomply” with regulations – whether to avoid liability for the conduct of their users or because overcompliance is simply cheaper or easier. Strict timelines for removal, for example, are one factor among many which may incentivize overcompliance. Numerous studies have highlighted overcompliance of intermediaries in response to intermediary liability laws.<sup>216</sup> Removal of legitimate content and removal of access for legitimate users as a result of overcompliance can constitute

<sup>211</sup> International Covenant on Civil and Political Rights, art. 19, para. 2.

<sup>212</sup> International Covenant on Civil and Political Rights, art. 19; Convention on the Rights of the Child, art. 13; African Charter on Human and Peoples’ Rights, art. 9; American Convention on Human Rights, art. 13; European Convention on Human Rights, art. 10.

<sup>213</sup> Human Rights Committee, general comment No. 34 (2011) on freedoms of opinion and expression, para. 2.

<sup>214</sup> Ibid., para. 3.

<sup>215</sup> Ibid., para. 7. See also Human Rights Committee, general comment No. 31 (2004) on the nature of the general legal obligation imposed on States Parties to the Covenant, para. 8. The Human Rights Committee does not further elaborate on the meaning of the phrase “to the extent that these Covenant rights are amenable to application between private persons or entities” in either of these general comments. However, the Human Rights Committee has applied the obligation to protect in relation to situations where certain public functions have been delegated to a private actor and in relation to rights that are commonly affected within private relationships, such as rights to privacy and non-discrimination, see Lottie Lane, “The horizontal effect of international human rights law in practice: a comparative analysis of general comments and jurisprudence of selected United Nations human rights treaty monitoring bodies”, *European Journal of Comparative Law and Governance*, vol. 5, No. 1 (March 2018), p. 43.

<sup>216</sup> For a review of such studies, see Daphne Keller, “Empirical evidence of “Over-removal” by Internet companies under intermediary liability laws”, Center for Internet and Society, Stanford Law School, 8 May 2020 (last update).

a restriction on freedom of expression. Additionally, actions such as surveillance, filtering, blocking and removal of communications can have indirect “chilling effects” on the exercise of freedom of expression.

## Right of peaceful assembly

The right of peaceful assembly,<sup>217</sup> “[t]ogether with other related rights, ... constitutes the very foundation of a system of participatory governance based on democracy, human rights, the rule of law and pluralism”.<sup>218</sup> It is closely related to other political rights such as freedom of association and freedom of political participation.<sup>219</sup> It is also important for the recognition and realization of a wide range of other rights, including economic, social and cultural rights.<sup>220</sup>

The way in which public assemblies are conducted and their context changes over time.<sup>221</sup> Emerging technologies present both opportunities and threats to the exercise of the right of peaceful assembly.<sup>222</sup> The Human Rights Committee notes that

Although the exercise of the right of peaceful assembly is normally understood to pertain to the physical gathering of persons, [the protection of the right of peaceful assembly under article 21 of the ICCPR] also extends to remote participation in, and organisation of, assemblies, for example online.<sup>223</sup>

The right of peaceful assembly also protects associated activities such as participants’ or organisers’ mobilization of resources, planning, dissemination of information about an upcoming event, communication between participants leading up to and during the assembly, and broadcasting of or from the assembly.<sup>224</sup> Many of these associated activities happen online or otherwise rely upon digital services.<sup>225</sup>

The right of peaceful assembly also entails positive duties of States to protect the exercise of this right from interference by third parties.<sup>226</sup> The Human Rights Council’s Special Rapporteur on the rights to freedom of peaceful assembly and of association has noted that:

In the digital age, the exercise of the rights of peaceful assembly and association has become largely dependent on business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms can affect these freedoms. Online platforms and social media companies, in particular, wield significant power over how both the right to freedom of peaceful assembly and the right to freedom of association are enjoyed and exercised.<sup>227</sup>

The Human Rights Committee has likewise noted that “increased private ownership and other forms of control of public accessible spaces and communication platforms” must inform a contemporary understanding of the right to peaceful assembly.<sup>228</sup>

<sup>217</sup> See International Covenant on Civil and Political Rights, art. 21; Convention on the Rights of the Child, art. 15; African Charter on Human and Peoples’ Rights, art. 11; American Convention on Human Rights, art. 15; European Convention on Human Rights, art. 11.

<sup>218</sup> Human Rights Committee, general comment No. 37 (2020), para. 1.

<sup>219</sup> Ibid., para. 9; A/HRC/44/24, para. 5. For freedom of association and the freedom of political participation, see International Covenant on Civil and Political Rights, arts. 22 and 25.

<sup>220</sup> Human Rights Committee, general comment No. 37 (2020), para. 2.

<sup>221</sup> Ibid., para. 10.

<sup>222</sup> Ibid.; A/HRC/41/41, para. 2.

<sup>223</sup> Human Rights Committee, general comment No. 37 (2020), para. 13. See also A/HRC/41/41; Human Rights Council resolution 38/7, para. 1; A/HRC/44/24, para. 5.

<sup>224</sup> Human Rights Committee, general comment No. 37 (2020), para. 33.

<sup>225</sup> Ibid., para. 34; A/HRC/44/24, paras. 7–8.

<sup>226</sup> Human Rights Committee, general comment No. 37 (2020), para. 24; A/HRC/41/41, para. 20.

<sup>227</sup> A/HRC/41/41, para. 17.

<sup>228</sup> Human Rights Committee, general comment No. 37 (2020), para. 10.

Actions such as surveillance, filtering, and blocking and removal of communications or access restrict the exercise of the right of peaceful assembly online.<sup>229</sup> In developing and evaluating policy measures to address wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online, States must take into account the effects that their action (or inaction) may have on the exercise of this right online. This is the case in relation to both liability-based and cooperation-based policy measures. It is also the case whether the effects on the exercise of the right of peaceful assembly are the direct result of the measures or the consequences of actions taken by intermediaries and others in response to or in the absence of such measures. In this context, the Human Rights Committee has noted that “States should ensure that the activities of Internet service providers and intermediaries do not unduly restrict assemblies or the privacy of assembly participants”.<sup>230</sup>

## Right to privacy

The right to privacy protects against arbitrary or unlawful interference with privacy, family, home or correspondence.<sup>231</sup> It protects against all such interferences, whether emanating from State authorities or from natural or legal persons.<sup>232</sup> The General Assembly has recognized that “the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society”.<sup>233</sup>

States must also protect the right to privacy online.<sup>234</sup> The development of information and communication technologies has enhanced the capacities of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse the right to privacy or other human rights.<sup>235</sup> Everything that is done online generates personal data, which is often sensitive. In 2014, the General Assembly expressed its deep concern at the negative impact of surveillance and interception of communications and collection of personal data on the exercise and enjoyment of human rights such as freedom of expression, particularly when carried out on a mass scale.<sup>236</sup> Interference with the right to privacy online can create a “chilling effect” on speech and economic activity online. Indeed, 45 per cent of respondents to one survey conducted in the United States indicated that privacy and security concerns had stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues online.<sup>237</sup>

Measures taken by States and intermediaries to address wildlife crime, falsified medical products-related crime, or trafficking in cultural property online have the potential to affect the exercise of the right to privacy. In particular, measures which involve surveillance, filtering, personal data requests or mandatory reporting of suspicions of illicit activity will impact upon users’ privacy. Direct and indirect effects on the exercise of the right to privacy must be considered by policymakers when developing and evaluating policy measures to address these crimes.

<sup>229</sup> A/HRC/44/24, paras. 17, 24–29.

<sup>230</sup> Human Rights Committee, general comment No. 37 (2020), para. 34.

<sup>231</sup> See International Covenant on Civil and Political Rights, art. 17; Convention on the Rights of the Child, art. 15; American Convention on Human Rights, art. 11; European Convention on Human Rights, art. 8.

<sup>232</sup> A/43/40, annex VI.

<sup>233</sup> General Assembly resolution 68/167, fifth preambular paragraph.

<sup>234</sup> *Ibid.*, para. 3.

<sup>235</sup> *Ibid.*, fourth preambular paragraph.

<sup>236</sup> *Ibid.*, tenth preambular paragraph.

<sup>237</sup> Rafi Goldberg, “Lack of trust in Internet privacy and security may deter economic and other online activities”, National Telecommunications and Information Administration, 13 May 2016.

## Right to effective remedy

The right to effective remedy<sup>238</sup> requires that States ensure that individuals have accessible and effective remedies to vindicate the violation of their human rights.<sup>239</sup> Cessation of an ongoing violation is an essential element of the right to an effective remedy.<sup>240</sup> It further requires that States make reparation to individuals whose rights have been violated.<sup>241</sup> Reparation generally entails adequate compensation and, where appropriate, may involve other measures such as restitution, rehabilitation and measures of satisfaction.<sup>242</sup> It may also require that measures be taken to prevent a recurrence of the violation.<sup>243</sup>

States must also ensure access to an effective remedy in relation to violations of human rights by businesses. Principle 25 of the United Nations Office of the High Commissioner for Human Rights' *Guiding Principles on Business and Human Rights*, endorsed by the Human Rights Council,<sup>244</sup> states that:

As part of their duty to protect against business related human rights abuse, States must take appropriate steps to ensure, through judicial administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy.<sup>245</sup>

The commentary to Principle 25 further notes “[u]nless States take appropriate steps to investigate, punish and redress business-related human rights abuses” the State duty to protect against violations of human rights “can be rendered weak or even meaningless”.<sup>246</sup> Furthermore, pursuant to Principle 22, where business enterprises identify that they have caused or contributed to adverse impacts, they should provide for or cooperate in their remediation through legitimate processes.

This chapter has identified several ways that the actions of online intermediaries can affect the exercise of freedom of expression, the right of peaceful assembly and the right to privacy. States must ensure that where such actions amount to an abuse of these or other human rights, that the individuals whose rights have been violated have access to effective remedy.

## PERMISSIBLE RESTRICTIONS TO HUMAN RIGHTS

This chapter has thus far considered some of the key human rights obligations of States relevant to wildlife crime, falsified medical products-related crime and trafficking in cultural property, as well as to policy measures aimed at addressing these crimes online. It has also considered how measures taken by States and online intermediaries can affect and restrict the exercise of human rights.

Restrictions on the exercise of human rights do not necessarily constitute violations of those human rights. Some (but not all) human rights may lawfully be restricted when certain circumstances are met. This section considers the question of when, under international human rights law, States can permissibly limit the exercise of human rights in relation to policies aimed at preventing and combating wildlife crime, falsified medical products-related crime and/or trafficking in cultural property.

<sup>238</sup> See International Covenant on Civil and Political Rights, art. 2, para. 3; European Convention on Human Rights, art. 13; American Convention on Human Rights, art. 25.

<sup>239</sup> Human Rights Committee, general comment No. 31 (2004), para. 15.

<sup>240</sup> Ibid.

<sup>241</sup> Ibid., para. 16.

<sup>242</sup> Ibid.

<sup>243</sup> Ibid., para. 17.

<sup>244</sup> Human Rights Council resolution 17/4, para. 1.

<sup>245</sup> Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework (A/HRC/17/31, annex, chap. III, sect. A, item 25).

<sup>246</sup> Ibid.



Whereas some human rights are absolute, meaning that they do not admit any limitation imposed by States,<sup>247</sup> non-absolute rights may be subject to restrictions when certain conditions are met. Provisions of human rights treaties sometimes expressly recognize that certain rights may be restricted in particular circumstances. This is the case for both freedom of expression and the right of peaceful assembly under ICCPR.<sup>248</sup>

In order for a restriction to a human right to be permissible under ICCPR, it must be prescribed by clear and accessible law,<sup>249</sup> serve a legitimate aim, and be necessary for meeting, and proportionate to, that legitimate aim.<sup>250</sup> It is the State in question that has the burden of proving that each of these requirements is met in relation to a restriction imposed on human rights.<sup>251</sup> Additionally, no provision of ICCPR or ICESCR may be relied upon to destroy any of the rights or freedoms contained therein, and no fundamental human rights recognized or existing in any State shall be restricted or derogated from on the pretext that one or both of these instruments do not recognize the right or recognize it to a lesser extent.<sup>252</sup>

The requirement that a law restricting the exercise of a right be clear and accessible law (in other words, the principle of legality) requires that the law establishing the restriction must be made accessible to the public and be formulated with sufficient clarity to enable an individual or business to regulate their conduct accordingly.<sup>253</sup> In the context of measures to prevent and combat wildlife crime, falsified medical products-related crime and trafficking in cultural property online, this requires that the obligations of online intermediaries to filter, restrict or remove content or to remove access of users be sufficiently clear.

The legitimate aim for which a right may be restricted depends upon the right in question. ICCPR provides that freedom of expression may be restricted for “respect of the rights or reputations of others” or for “the protection of national security or of public order (ordre public), or of public health or morals”.<sup>254</sup> For the right of peaceful assembly, it provides that that the right may be restricted “in the interests of national security of public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others”. In contrast, permissible restrictions to the right to privacy are not enumerated by ICCPR, though it is accepted that the applicable permissible restrictions to this right are likely to be very similar to those of other ICCPR rights, such as freedom of expression and the right of peaceful assembly.<sup>255</sup>

Preventing and combating wildlife crime, falsified medical products-related crime and trafficking in cultural property online are legitimate aims. These ends may be seen to protect public order or public health. As was shown earlier in this chapter, they may also contribute to help protect the rights of others, such as the right to health, the right to life and the right to take part in cultural life.

Having a legitimate aim is, however, not enough for restrictions to human rights to be permissible. The restrictions imposed must also be necessary and proportionate to this aim. In this regard, the Committee on Economic, Social and Cultural Rights has expressed its concern about the right to health and issues of public health being used as grounds for limiting the exercise of other human rights and reiterated the need for

<sup>247</sup> Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, 3rd ed. (Oxford, Oxford University Press, 2013), para. 1.82.

<sup>248</sup> See International Covenant on Civil and Political Rights, art. 19, para. 2 and art. 20.

<sup>249</sup> Human Rights Committee, general comment No. 34 (2011), para. 25. See further Oscar M. Garibaldi, “General limitations on human rights: the principle of legality”, *Harvard International Law Journal*, vol. 17, No. 3 (1976), p. 503.

<sup>250</sup> Human Rights Committee, general comment No. 31 (2004), para. 6; Human Rights Committee, general comment No. 34 (2011), para. 22; Human Rights Council resolution 15/21, para. 4.

<sup>251</sup> Human Rights Committee, general comment No. 34 (2011), on freedoms of opinion and expression, para. 35; Committee on Economic, Social and Cultural Rights, general comment No. 14 (2000), para. 28.

<sup>252</sup> International Covenant on Civil and Political Rights, art. 5; International Covenant on Economic, Social and Cultural Rights, art. 5.

<sup>253</sup> Human Rights Committee, general comment No. 34 (2011), on freedoms of opinion and expression, para. 25.

<sup>254</sup> International Covenant on Civil and Political Rights, art. 19, para. 3.

<sup>255</sup> Joseph and Castan, *The International Covenant on Civil and Political Rights*, para. 16.12.

measures to be necessary and proportionate.<sup>256</sup> The Committee on Economic, Social and Cultural Rights has similarly reiterated that the right to take part in cultural life may not be interpreted as implying any right to limit other rights and freedoms recognized in ICESCR to a greater extent than is provided for therein.<sup>257</sup> Whether restrictions are necessary and proportionate must be assessed on a case-by-case basis. Nevertheless, it is possible to make some general observations of relevance to measures which seek to prevent and combat wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online.

First, the test of necessity will not be met where the legitimate aim could have been achieved in other ways that do not restrict human rights.<sup>258</sup> Accordingly, States are obliged to investigate alternatives that would not involve restrictions to human rights before introducing legislation that would have this effect.

Second, measures that are ineffective or counterproductive cannot be said to be necessary to achieve a legitimate aim. For example, it was noted in chapter 3 that measures may be ineffective or counterproductive when they provide incentives to online intermediaries to take actions that inadvertently have the consequence of obstructing law enforcement investigations, such as removal of content. This underscores the need for States to not only carefully design policy measures but to monitor and evaluate them on an ongoing basis to determine whether they are achieving their aims and to adapt and revise them as necessary.

Third, the test of proportionality requires that restrictions be appropriate to achieve their protective function; that they be the least intrusive alternative among those which might achieve the desired result; and that they be proportionate to the interest to be protected.<sup>259</sup> Each of these considerations must be taken into account by States in developing and evaluating policy measures to address the crimes discussed in this paper. It is again important to note that States have human rights obligations not only in relation to the measures that they directly take but also in relation to the conduct of third parties. Accordingly, when considering whether State measures are proportionate to their aim, the human rights effects of actions taken by online intermediaries pursuant to these measures will also be relevant.

Fourth, what is necessary and proportionate can and will change over time as the nature of the crimes addressed by this paper and the technologies both used to commit these crimes and available for preventing them continue to develop. This too underscores the need for States to monitor, evaluate and adapt policy measures.

Finally, the principle of proportionality must not only be respected by the law establishing the restriction, but also by the administrative and judicial authorities which apply the law.<sup>260</sup>

## CONCLUSION

This chapter has explored some of the key human rights dimensions of policymaking to address wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online. It has shown how each of these crimes can threaten the exercise of human rights such as the right to health, the right to life and the right to take part in cultural life. It has further shown how States have positive duties under international human rights law to prevent third parties from interfering with these rights, which require States to take action to prevent and combat these crimes.

This chapter has examined the human rights implications of policy measures to address these crimes online. It has shown how actions taken by States and online intermediaries can interfere with freedom of

<sup>256</sup> Committee on Economic, Social and Cultural Rights, general comment No. 14 (2000), para. 28.

<sup>257</sup> Committee on Economic, Social and Cultural Rights, general comment No. 21 (2009), para. 20.

<sup>258</sup> Human Rights Committee, general comment No. 34 (2011), para. 33.

<sup>259</sup> *Ibid.*, para. 34; Human Rights Committee, general comment No. 27 (1999) on freedom of movement, para. 14.

<sup>260</sup> Human Rights Committee, general comment No. 34 (2011), para. 34; Human Rights Committee, general comment No. 27 (1999), para. 15.

expression, the right of peaceful assembly and the right to privacy and underscored the need for the right to effective remedy to be upheld.

States must develop policy approaches to addressing wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online which respect all human rights. In doing so, States may need to restrict the exercise of particular human rights to protect other human rights or other legitimate aims. This chapter has outlined the requirements of international human rights law for permissible restrictions to human rights. To be permissible, restrictions must be prescribed by clear and accessible law, serve a legitimate aim, and be necessary for meeting, and proportionate to, that legitimate aim.<sup>261</sup>

---

<sup>261</sup> For a further resource concerning the application of international human rights law online, see “Necessary and proportionate: International Principles on the Application of Human Rights to Communications Surveillance” (May 2014). See also “Manila Principles on Intermediary Liability: Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation – a Global Civil Society initiative”, version 1.0 (March 2015); The Santa Clara Principles on Transparency and Accountability in Content Moderation, available at <https://santaclaraprinciples.org/>.







---

# CONCLUSION

This issue paper has considered, from the perspective of State policymaking, the role of online intermediaries in preventing and combating three forms of serious crime online: wildlife crime, falsified medical products-related crime, and trafficking in cultural property.

The digitization of society has offered significant economic and social opportunities but it has also created opportunities for organized criminal activities such as online trafficking in wildlife products, falsified medical products and cultural property. States must understand the nature of these threats in order to effectively address them. In chapter 1, this paper provided an overview of the nature of and threats posed by wildlife crime, falsified medical products-related crime, and trafficking in cultural property. Each of these crime types is serious in terms of the harms they cause and their geographic and economic scale. The seriousness of these crimes has been repeatedly recognized by the international community. Furthermore, each of these crimes are increasingly being committed online.

Effective policymaking online must also be based on a solid understanding of how the Internet operates and the multitude of online intermediaries. Chapter 2 of this paper provided an introduction to the Internet, a brief overview of some key online intermediaries and their relevance to law enforcement and an explanation of the nature of relations between online intermediaries and their users. It showed that individuals and organizations rely on a complex chain of online intermediaries to access and use the Internet, which may be based in different jurisdictions and which have differing capacities to take action to address the unlawful activity of their users.

Approaches to preventing and combating wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online must effectively take into account the interests of the public, including both individuals and businesses, as well as online intermediaries themselves. Chapter 3 gave an overview of the interests of each of these key stakeholders. It showed that the online ecosystem is a complex web of overlapping interests and needs. It further showed that the interests of stakeholders are multiple and can pull in different directions, both between and within groups of stakeholders.

Policymakers seeking to address wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online should also understand the various policy options available to do so, their impacts on each of these crime types and their potential counterproductive effects. In chapter 4, this paper showed that the toolkit of policymakers in addressing wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online is varied and complex. It examined key considerations and issues relevant to two broad categories of policy measures: cooperation- and liability-based approaches. It further highlighted the importance of transparency and monitoring, evaluating and adapting measures.

Policy approaches should seek to provide online intermediaries with the right balance of incentives – to effectively support the State's efforts to prevent and combat these crimes in a manner which is proportionate, which does not infringe upon the exercise of users' rights, and which allows legitimate online activities to flourish. In chapter 5, human rights dimensions of policymaking in respect of wildlife crime, falsified medical products-related crime and trafficking in cultural property online were examined. These included both the human rights implications of these crimes and actions taken by States and online intermediaries to fight these crimes online. It emphasized the responsibility of States to adequately assess and take into consideration the human rights implications of policymaking, including actions taken by online intermediaries

and others in response to government policies. It further set out the international human rights law framework under which policies seeking to prevent and combat wildlife crime, falsified medical products-related crime and/or trafficking in cultural property online must be assessed.

In analysing these issues, this paper has not provided ready answers for policymakers on how to solve these problems. Rather, this paper has sought to map the key stakeholders, interests, issues and considerations relevant to policymakers in developing measures to prevent and combat the commission of these crimes online. The correct approach for each State to take will also vary in accordance with a multitude of local factors. Furthermore, more research is needed into the nature and scale of these crime types online, the effectiveness of the variety of policy options in preventing and combating them, and the potential negative side effects of these policy options, including on the exercise of human rights and legitimate online commerce. It is hoped that this issue paper will contribute to a stronger knowledge base for future research and policy discussions.







# UNODC

United Nations Office on Drugs and Crime