ARTICLE 19 and Human Rights Watch's Comments on the Draft Text of the UN Cybercrime Convention

Submitted to the United Nations General Assembly Ad hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes in its sixth session

August 2023

Table of Contents

Introduction

1. Human Rights Watch (HRW) and ARTICLE 19 welcome the opportunity to provide observations and recommendations to the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its draft text of the proposed convention (hereafter "the Draft Text" or "the Proposed Convention").[1] We recognize that the Committee has worked extensively on the Draft Text and that some of the most problematic proposals have been rightly excluded. Despite this progress, much more work is needed to safeguard human rights in the treaty.

2. Our main concerns with the Draft Text are:

    - Its near unlimited scope, which risks both substantively criminalizing acts beyond core cybercrimes, and disproportionately increasing policing powers and cooperation for those offences.
    - Criminalization of acts that risk:
        - Encroaching on the rights of children, in particular lesbian, gay, bisexual, and transgender (LGBT) children, including adolescents, seeking information about sexual and reproductive health and rights, sexual and gender diversity, and other topics that fall under the rubric of comprehensive sexuality education.
        - Encroaching on the rights of survivors of online gender-based violence, including people targeted with non-consensual dissemination of intimate images.
        - Lack of adequate protections for the legitimate work of civil society organizations, journalists, security researchers, and whistleblowers, as well as for protected expression that has scientific, artistic, or literary value.
    - Increased policing powers and cooperation beyond core cybercrimes, without adequate human rights safeguards.
    - Inadequate safeguards in the general human rights provisions, which is particularly concerning in light of the nature and scope of this Proposed Convention.

3. Our main recommendations are as follows:

    - **Recommendation 1: Delete Article 17 in its entirety. [6-14]**
    - **Recommendation 2: Delete Paragraph (3) of the preamble. [15-17]**
    - **Recommendation 3: Amend Article 22 to include proportionality and prevent it from applying to multi-national platforms that have not committed an offence under Article 6 to 16. [18-19]**
    - **Recommendation 4: Delete Article 13 in its entirety. If the provision is nonetheless retained, amend Article 13 to exclude conduct that does not unduly risk harm to a child and has a legitimate purpose and to limit the risk of criminalizing non-exploitive conduct of children, an unduly expanded range of prohibited content, and the creation, possession or sharing of prohibited content in non-exploitive circumstances [due to a lack of context]. [21-27]**
    - **Recommendation 5: Delete Article 14 in its entirety. If the provision is nonetheless retained, amend Article 14 to limit the risk of criminalizing activities of children who are above the age of consent but still captured**

[1] United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, "Draft Text of the Convention," A/AC.291/22, May 29, 2023, https://undocs.org/en/A/AC.291/22 (accessed August 20, 2023).

by the Draft Text, of criminalizing people seeking or imparting information regarding sexual and reproductive health, and of the use of these provisions to discriminate against same-sex interactions. [25-27]

- Recommendation 6: Consider the appropriateness of including Article 15. If the provision is retained, amend Article 15 to mitigate the risk of criminalizing survivors particularly where the perpetrator is an authority figure, to center the lack of freely given consent, to criminalize the non-consensual capturing of intimate images and to exempt conduct that is a matter of public interest or for a legitimate purpose related to the administration of justice. [28-31]
- Recommendation 7: Amend Articles 6-10 so that: fraudulent or otherwise malicious intent conduct must result in serious harm or damage in order to be criminalized, bypassing technical safeguards is a core element of each criminal act, and a public interest exception is included. [32-33]
- Recommendation 8: Amend Article 5 so that it ensures the Proposed Convention does not threaten human rights and to mainstream a gender perspective and take into consideration the circumstances of persons and groups who face discrimination and marginalization, amend the preamble to add Paragraph 9*bis* recognizing the important role of civil society, the Office of the High Commissioner for Human Rights and the international human rights mechanisms in the implementation of the Proposed Convention, and amend Paragraphs 11 and 12 of the preamble so that international human rights law and standards are reflected. [35-38]
- Recommendation 9: Amend Articles 21, 23, 24 and 35 to align the Draft Text's core safeguards regarding due process, investigative powers and international cooperation with international human rights law including through incorporation of the principles of legality, necessity, proportionality, and dual criminality. [39-43]
- Recommendation 10: Delete Articles 23(2)(b) and 23(2)(c), and amend Articles 35(1), 40(1), 40(4), 41(1), 45(2), 47(1) and 47(1)(b)(if retained) so that international cooperation and mutual legal assistance are limited to in scope to offences established in accordance with Articles 6 to 16 of the Draft Text. [45-50]
- Recommendation 11: Amend Article 40(4) to exclude proactive cross-border disclosure of personal data, amend Articles 42-46 so that mutual legal assistance is carried out in accordance with safeguards and limitations set out in Chapter IV of the Draft Text, amend Articles 44 and 45 to allow refusal of requests for mutual legal assistance on the basis of the grounds contained in Article 40(21), remove Articles 47(1)(b) and (c), remove Article 47(1)(g) or, at minimum, amend it to exclude any sharing of personal data, amend Article 47(1)(d) to remove information sharing regarding the use of privacy-enhancing tools, and amend Article 54 to incorporate safeguards against human rights abuses. [51-56]

4. We note that more extensive commentary on chapters related to procedural measures and law enforcement, as well as international cooperation by the Electronic Frontier Foundation (EFF) and Privacy International (PI) and by ARTICLE 19 is available.[2]

[2] Privacy International and Electronic Frontier Foundation, "Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V & VII, July 2023," https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Privacy_Intl_EFF.pdf. (accessed August 20, 2023); ARTICLE 19, "Comments on the "Zero Draft" of the UN Cybercrime Convention," July 2023, https://www.article19.org/wp-content/uploads/2023/07/ARTICLE-19-analysis-of-the-Cybercrime-Convention-Zero-Draft-Final.pdf (accessed August 20, 2023).

The Draft Text's near-unlimited scope undermines human rights

5. Human Rights Watch and ARTICLE 19 appreciate that the drafting process has made some progress in eliminating substantive offences that are "cyber-enabled" rather than "cyber-dependent", in particular those which would have restricted freedom of expression and other human rights. However, the Draft Text continues to be problematic in scope, criminalizing activities that do not constitute "core" cybercrimes while proposing chapters on investigative powers and international cooperation that apply to all serious crimes. Article 17 of the Draft Text is a central concern in that it extends an indeterminate range of offences to digital contexts without modification, including some offences that pose a direct threat to freedom of expression.

Article 17: Substantive offences should be clearly articulated in the Proposed Convention

Recommendation 1: Delete Article 17 in its entirety. [6-14]

6. The Draft Text continues to lack a coherent articulation of what does or does not constitute a cybercrime. While it initially appears to limit the number of substantive offences to Articles 6 through 16, language throughout the Draft Text indicates the scope is far from limited to those offences. Rather, the scope is explicitly open-ended.

7. By virtue of Article 17, any offence included in a binding treaty becomes a cybercrime, an expanding list of offences that already includes everything from drug offences to smuggling of migrants.

8. A complete understanding of the challenges raised by this provision would require a detailed assessment of numerous existing treaties. This assessment is difficult to carry out at the present stage as it is not clear what pre-existing treaties are covered. Article 17 is not, for example, limited to treaties duly registered in accordance with Article 102 of the UN Charter and may be viewed by some parties as applying to instruments ranging from binding regional or even bilateral agreements to trade agreements. The full implications of Article 17 cannot be understood because as currently drafted, it could also apply to future treaties including where those future treaties deliberately avoid applying their provisions to online environments.

9. The principle underpinning Article 17 essentially establishes that if technology is used in the commission of a crime, then it constitutes a cybercrime. This approach is particularly concerning in light of the propensity of States to use cybercrime measures against civil society organizations and human rights defenders.[3] The treaty should clearly articulate the harm it is addressing and only include specified "core" cybercrimes where communications networks are an integral component of the criminal act. Its procedural powers and international cooperation chapters should similarly be limited to specific investigations and prosecutions of these core cybercrimes.

10. We question the utility of this provision. Most offences in pre-existing treaties are not inherently limited to physical contexts and, absent practical barriers that suggest a given provision is ill-suited to criminalizing online behavior, would already apply. If the provision is intended to be redundant in nature, it creates challenges by embedding overlapping obligations regarding the online dimensions of offences in one Convention while both online and real-world offences remain governed by the underlying treaties in question. If the provision is intended to extend

[3] UN General Assembly, "Implementing the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms through providing a safe and enabling environment for human rights defenders and ensuring their protection," Resolution 74/146, A/RES/74/146, https://undocs.org/en/A/RES/74/146 (accessed August 20, 2023); Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Special Rapporteur on the rights to freedom of peace and assembly and of association, Special Rapporteur on the situation of human rights defenders, and Special Rapporteur on the right to privacy, "Libya: Comments on the Anti-Cybercrime Law," LBY 3/2022, March 31, 2022, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=27150 (accessed August 20, 2023); "Abuse of Cybercrime Measures Taints UN Talks," Human Rights Watch news release, May 5, 2021, https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks; Association for Progressive Communications, "GIS Watch 2017: Unshackling Expression: A Study of Laws Criminalising Expression Online in Asia," 2017, https://www.giswatch.org/sites/default/files/giswspecial2017_web.pdf (accessed August 20, 2023).

existing offences to online environments despite practical barriers it does so without consideration of the different challenges that can arise in digital contexts and despite a lack of consensus regarding the degree to which these offences should apply online. Indeed, reliance on Article 17 will only be necessary in the absence of consensus regarding the online dimensions of existing treaty obligations. This blunt approach can lead to significant unintended consequences including erosion of human rights and can bypass many of the explicit limitations adopted in the Proposed Convention as well as in the underlying treaties that Article 17 would extend to the online environment. We provide some indicative examples of these challenges below.

11. The Council of Europe Convention on Cybercrime (the Budapest Convention) explicitly excluded attempts to incorporate a range of content-related offences as these raised significant freedom of expression concerns and therefore could not generate consensus.[4] Among these attempts were proposals to extend racist and xenophobic speech offences included in the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) to the online ecosystem,[5] which were excluded from the Budapest Convention and instead negotiated in a separate protocol criminalizing racist and xenophobic speech committed through computer systems that has enjoyed more limited adoption.[6] We note that under international human rights law, any advocacy of national racial or religious hatred that constitutes incitement to discrimination, hostility, or violence should be prohibited by law. However, States are not obligated to criminalize such expression.[7] The criminalization of racist and hate speech, particularly in online environments, is frequently weaponized by States seeking to attack online expression by civil society groups and particularly groups critical of governments.[8] Compelling States to extend ICERD offences to the Internet without modification or safeguard poses a direct risk to human rights.

12. In adopting racist and xenophobic speech offences to the online ecosystem, the optional Council of Europe protocol incorporated a number of specific safeguards necessary to adapt the provision to digital networks.[9] By

[4] "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems," ETS No.189, January 28, 2003, https://rm.coe.int/1680989b1c (accessed August 20, 2023). We note that content offences in general have historically raised significant freedom of expression concerns, and these are heightened with respect to the online dimensions and treatment of these offences. See Office of the High Commissioner for Human Rights (OHCHR), "Key-messages relating to a comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes," January 17, 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf, (accessed August 20, 2023), p. 2.

[5] ICERD has 182 States Parties. An additional 3 States have signed ICERD. See "Status of Ratification Interactive Dashboard: Ratification of 18 International Human Rights Treaties," OHCHR website, accessed August 202, 2023, https://indicators.ohchr.org/. International Convention on Eliminating All Forms of Racial Discrimination (ICERD), adopted December 21, 1965, G.A. Res 2106 (XX)A annex, 20 UN G.A.O.R. Supp. (No. 14) 47, U.N. Doc. A/RES/2106(XX)[A] Annex, (1966), 660 U.N.T.S. 195, entered into force January 4, 1969, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial (accessed August 20, 2023).

[6] "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems," ETS No.189, January 28, 2003, https://rm.coe.int/1680989b1c (accessed August 20, 2023).

[7] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/74/486, October 9, 2019, https://undocs.org/en/A/74/486, (accessed August 20, 2023), para. 8.

[8] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/67/357, September 7, 2012, https://undocs.org/en/A/67/357, (accessed August 20, 2023), paras. 51-52; UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/74/486, October 9, 2019, https://undocs.org/en/A/74/486, (accessed August 20, 2023), paras. 1 and 4; ARTICLE 19, "Central Asia: Freedom of expression online," January 1, 2022, https://www.article19.org/central-asia-freedom-of-expression-online/ (accessed August 20, 2023); "How are the Authorities in Central Asia Trying to Control the Internet?," Human Rights Watch news release, November 18, 2021, https://www.hrw.org/news/2021/11/18/how-are-authorities-central-asia-trying-control-internet; Human Rights Watch, *False Freedom: Online Censorship in the Middle East and North Africa* (New York: Human Rights Watch, 2005), https://www.hrw.org/report/2005/11/14/false-freedom/online-censorship-middle-east-and-north-africa; Human Rights Watch, *Online and On All Fronts Russia's Assault on Freedom of Expression* (New York: Human Rights Watch, 2017), https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression; Association for Progressive Communications, "GIS Watch 2017: Unshackling Expression: A Study of Laws Criminalising Expression Online in Asia," 2017, https://www.giswatch.org/sites/default/files/giswspecial2017_web.pdf (accessed August 20, 2023).

[9] For example, a "without right" qualification was added, in part to make clear that "Legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices not be criminalized." See "Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer

virtue of Article 17, hate speech offences included in instruments such as ICERD could be extended to the online environment without any of these safeguards in place.[10]

13. Article 17 also causes challenges for States who may wish to reserve all or part of the online aspect of an ICERD offence. The Council of Europe optional protocol explicitly states that a Party may reserve the right not to attach criminal liability to the distribution of racist and xenophobic material to the public through a computer system, where the material advocates, promotes, or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available or doing so would be incompatible with principles concerning freedom of expression established by its national legal system.[11] As the obligation to extend ICERD offences to online contexts would arise from Article 17 of the current Convention and not from ICERD itself, comparable reservations would need to be consistent with this Proposed Convention rather than with Article 20 of ICERD.[12] Similar challenges would arise in relation to reservations in relation to any offences housed in other treaties and extended to the online environment by virtue of Article 17.

14. A number of other offences in existing treaties will also be problematic if extended to the online environment without modification. For example, treaties that were negotiated decades ago to address terrorism-related physical attacks are not an effective means of addressing this complexity and should not be forcefully stretched to address cyberattacks by virtue of Article 17. Offences criminalizing physical attacks on civil aviation have, for example, been adopted in a patchwork of instruments.[13] Each of these instruments has different levels of adoption amongst State Parties and each establishes different thresholds for intent and jurisdiction while many do not address these criteria at all.[14] Where thresholds are established, many are designed to address physical attacks and are ill-suited to addressing cyber threats. The conduct criminalized by these civil aviation instruments and extended to digital contexts through Article 17 will frequently overlap imperfectly with offences set out in Articles 6-10 of the Draft Text,[15] but without the calibration and limitations negotiated in these proposed provisions. Limitations on criminal intent adopted in Articles 6-10 of the Draft Text will not apply to cyber threats criminalized under Article 17, nor would conditions established in Articles 18-22 of the Draft Text to address jurisdiction, establish the proper scope of corporate liability and impose due process safeguards.[16] We therefore recommend the deletion of Article 17 in its entirety.

systems," ETS No.189, January 28, 2003, https://rm.coe.int/1680989b1c (accessed August 20, 2023). The Draft Text adopts a similarly narrow scope of liability for private sector actors such as service providers. Article 18 is limited to imposing liability for participation that is of a criminal character (e.g. aiding and abetting, instigation, assisting, etc). But Article 18 does not apply to offences adopted by virtue of Article 17.

[10] ICERD, art 4(a), adopted by the United Nations General Assembly in 1965, requires States Parties to criminalize the "dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin."

[11] "Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems," ETS No. 189, January 28, 2003, https://rm.coe.int/168008160f, (accessed August 20, 2023), paras. 2 and 3.

[12] ICERD, art 20(2): "A reservation incompatible with the object and purpose of this Convention shall not be permitted, nor shall a reservation the effect of which would inhibit the operation of any of the bodies established by this Convention be allowed. A reservation shall be considered incompatible or inhibitive if at least two thirds of the States Parties to this Convention object to it."

[13] International Civil Aviation Organization (ICAO) Secretariat Study Group on Cybersecurity, "Draft Study on the Applicability of International Air Law Instruments to Cyber Threats against Civil Aviation," https://www.icao.int/Meetings/LC38/References/SSGC-RSGLEG%20Draft%20Study%20on%20the%20Applicability%20of%20IAL%20to%20Cyber%20Threats%20Against%20Civil%20Aviation.pdf, (accessed August 20, 2023), para. 1.4.3.

[14] Ibid.

[15] Ibid, paras. 4.5.1-4.5.2; Council of Europe Cybercrime Convention Committee (T-CY), "Aspects of Terrorism covered by the Budapest Convention," T-CY (2016)11, November 15, 2016, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680bd640 (accessed August 20, 2023).

[16] Articles 18-22 do not apply to offences adopted by operation of Article 17.

Preamble, Paragraph 3: Remove unrelated offences

Recommendation 2: Delete Paragraph (3) of the preamble. [15-17]

15. The inclusion of the list of issues of concern in Paragraph (3) creates a disconnect between the preamble and the criminal offences contained in Chapter I, which the Draft Text aims to address.

16. Paragraph (3) addresses cyber-enabled offences "related to terrorism, trafficking in persons, smuggling of migrants, illicit manufacturing of and trafficking in firearms," which in our view have no place in this treaty. Paragraph (3) should be removed as it only creates confusion and ambiguity as to the scope of the Draft Text.

17. The reference to terrorism is particularly concerning, as there is no universally agreed upon definition of terrorism under international law. States have often leveraged this highly subjective term to justify repressive measures that illegitimately and disproportionately restrict the rights to free expression, opinion and belief, including peaceful dissent.[17] A June 2023 joint global study by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism found widespread and systematic abuse of civil society and shrinking of civic space through laws and measures ostensibly aimed at countering terrorism..[18] Absent a clear, narrow definition of terrorism that comports with international human rights standards, Paragraph (3) risks perpetuating these and other human rights violations by expanding the application of already overbroad counterterorrism laws to cybercrime.

Article 22: Scope of Jurisdiction measures will have negative human rights implications

Recommendation 3: Amend Article 22 to include proportionality and prevent it from applying to multi-national platforms that have not committed an offence under Article 6 to 16. [18-19]

> 1. Each State Party shall adopt such measures as may be necessary <u>and proportionate</u> to establish its jurisdiction over the offences established in accordance with articles 6 to 16 of this Convention when:
>
> …
>
> <u>6 *bis*. This Article does not apply to any legal person who has committed no offence under Articles 6 to 16 or may be held liable for the commission of such offences in accordance with Article 18.</u>

18. It is common practice for States to enact cohesive regulation of internet and communication platforms, including through cybercrime laws. These regimes increasingly include severe frameworks for asserting jurisdiction over multinational platforms. Common features of these frameworks include licensing requirements for online

[17] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/40/52, March 1, 2019, https://undocs.org/en/A/HRC/40/52 (accessed August 20, 2023); ARTICLE 19, "Comments on the Consolidated Negotiating Document on the Elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes," January 2023, https://www.article19.org/wp-content/uploads/2023/01/ARTICLE-19-analysis-of-the-Cybercrime-Convention-Negotiating-Document-January-2023.pdf (accessed August 20, 2023); "Statement to the Ad Hoc Committee on Cybercrime," Human Rights Watch, March 1, 2022, https://www.hrw.org/news/2022/03/01/human-rights-watchs-statement-ad-hoc-committee-cybercrime; Letta Tayler, "India's Abuses at Home Raise Concerns About Its Global Counterterrorism Role," *Just Security*, October 27, 2022, https://www.justsecurity.org/83787/indias-abuses-at-home-raise-concerns-about-its-global-counterterrorism-role/ (accessed August 20, 2023); Human Rights Watch, *In a Legal Black Hole: Sri Lanka's Failure to Reform the Prevention of Terrorism Act* (New York: Human Rights Watch, 2022), https://www.hrw.org/report/2022/02/07/legal-black-hole/sri-lankas-failure-reform-prevention-terrorism-act; Fionnuala Ní Aoláin, "Abusive "Counterterrorism" Crackdowns Choke Independent Civil Society in the Middle East," *Just Security*, August 25, 2022, https://www.justsecurity.org/82813/abusive-counterterrorism-crackdowns-choke-independent-civil-society-in-the-middle-east/ (accessed August 20, 2023); "Saudi Arabia: New Counterterrorism Law Enables Abuse," Human Rights Watch news release, November 23, 2017, https://www.hrw.org/news/2017/11/23/saudi-arabia-new-counterterrorism-law-enables-abuse (accessed August 20, 2023); Nadim Houry, "France's Creeping Terrorism Laws Restricting Free Speech," *Just Security*, May 30, 2018, https://www.justsecurity.org/57118/frances-creeping-terrorism-laws-restricting-free-speech/ (accessed August 20, 2023).

[18] United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "Global Study on the Impact of Counter-Terrorism on Civil Society & Civic Space," https://unglobalstudy.wpengine.com/wp-content/uploads/2023/06/SRCT_GlobalStudy.pdf (accessed August 20, 2023).

platforms, local presence and data localization requirements, the imposition of heavy fines, and the power to block or throttle platforms that refuse to comply with local laws.[19] Article 22 obligates State Parties to take "measures as may be necessary" to establish jurisdiction over cybercrime offences included in the Proposed Convention. The provision includes no safeguards or restrictions on what measures might be considered excessive,[20] and may be relied upon by States to justify practices that are incompatible with human rights when asserting investigative jurisdiction.[21] Questions regarding when jurisdiction over multi-national platforms and their subsidiaries can be asserted in cross-border investigations remain difficult to resolve with no clear consensus and should not be addressed through this Proposed Convention.[22]

19. In addition to being inherently problematic for failing to safeguard against the adoption of jurisdiction-conferring mechanisms that are incompatible with human rights, Article 22 is also an avenue to the enforcement of a range of "cybercrime" offences that amount to flagrant human rights abuses. By treating any conduct that might occur on a digital network as a potential "cybercrime" under Article 17, the Proposed Convention legitimizes an all-encompassing approach that invites States to address their own national priorities when enacting comprehensive cybercrime regimes. Often this list will include problematic "public morality", "undermining national unity", or "false news/disinformation" offences that are incompatible with the right to non-discrimination and the freedom of expression and association as part and parcel of a broader cybercrime package. A number of countries, for example, have criminalized expression around gender and sexuality under the guise of 'cybercrime', while other countries use cybercrime laws to punish peaceful protestors and political dissidents.[23] While Article 22 is limited in application to offences "established in accordance with Articles 6 to 16 of this Convention", in practice once these measures are used to compel jurisdiction over multi-national platforms States will have jurisdiction to investigate and enforce their entire suite of cybercrime offences established under national law. Article 22 is therefore problematic to the extent it facilitates investigation and enforcement of cybercrime offences that are incompatible with human rights by legitimizing disproportionate means of enforcing jurisdiction against multi-national platforms. The Proposed Convention's provisions should

[19] ARTICLE 19, "New Internet Law in Turkey Will Threaten Freedom of Expression," July 18, 2020, https://www.article19.org/resources/turkey-new-internet-law-threatens-freedom-of-expression-online/ (accessed July 18, 2023); ARTICLE 19, "New Censorship Threat with Elections Looming," October 14, 2022, https://www.article19.org/resources/turkey-dangerous-dystopian-new-legal-amendments/ (accessed July 18, 2023); "Indonesia: Suspend, Revise New Internet Regulation," Human Rights Watch news release, May 21, 2021, https://www.hrw.org/news/2021/05/21/indonesia-suspend-revise-new-internet-regulation; "Vietnam: Withdraw Problematic Cyber Security Law," Human Rights Watch news release, June 7, 2018, https://www.hrw.org/news/2018/06/07/vietnam-withdraw-problematic-cyber-security-law; "Jordan: Scrap Draconian Cybercrimes Bill," Human Rights Watch news release, July 24, 2023, https://www.hrw.org/news/2023/07/24/jordan-scrap-draconian-cybercrimes-bill.

[20] Draft Text, art. 22.

[21] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, May 11, 2016, https://undocs.org/en/A/HRC/32/38, (accessed August 20, 2023), paras. 40 and 61; UN Human Rights Council, Report of the Office of the High Commissioner for Human Rights on Internet Shutdowns: trends, causes, legal implications and impacts on a range of human rights, A/HRC/50/55, May 13, 2022, https://undocs.org/en/A/HRC/50/55 (accessed August 20, 2023). See also UN Human Rights Committee, General Comment No. 34, Freedoms of opinion and expression, CCPR/C/GC/34, 2011, https://undocs.org/en/CCPR/C/GC/34 (accessed August 20, 2023), para. 39.

[22] See, for example, *Microsoft v. United States*, 829 F.3d 197, United State Court of Appeals Second Circuit, July 14, 2016, https://casetext.com/case/microsoft-corp-v-united-states-in-re-a-warrant-to-search-a-certain-endashmail-account-controlled-maintained-by-microsoft-corp (accessed August 20, 2023); United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), "The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspective," January 2022, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf (accessed August 20, 2023), pp. 17-18.

[23] "Abuse of Cybercrime Measures Taints UN Talks," Human Rights Watch news release, May 5, 2021, https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks (accessed August 20, 2023); Afsaneh Rigot, "Digital Crime Scenes," Berkman Klein Center, March 7, 2022, https://cyber.harvard.edu/publication/2022/digital-crime-scenes (accessed July 24, 2023); Human Rights Watch, *"All This Terror Because of a Photo:" Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa* (New York: Human Rights Watch, 2023), https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt (accessed August 20, 2023); "Jordan's New Cybercrime Law is a Disaster for LGBT People," Human Rights Watch news release, August 14, 2023, https://www.hrw.org/news/2023/08/14/jordans-new-cybercrime-law-disaster-lgbt-people (accessed August 20, 2023); Association for Progressive Communications, "Unshackling Expression: A Study of Laws Criminalising Expression Online in Asia," 2017, https://www.giswatch.org/sites/default/files/giswspecial2017_web.pdf (accessed August 20, 2023).

foreclose foreseeable abuses of human rights in its implementation, and Article 22 should be amended to mitigate these risks.[24]

The Draft Text's criminal offences pose a threat to human rights

20. A number of the criminal offences contained in Chapter II threaten human rights. Articles 13 and 14 in particular may unduly restrict the rights of children and freedom of expression more generally. Article 15 could undermine the rights of survivors of technology-facilitated gender-based violence. The core cybercrime offences (Articles 6-10) lack critical safeguards to limit their misuse against whistleblowers, security researchers, and others.

Articles 13 and 14: Avoid unduly restricting the rights of children and freedom of expression more generally

Recommendation 4: Delete Article 13 in its entirety. If the provision is nonetheless retained, amend Article 13 to exclude conduct that does not unduly risk harm to a child and has a legitimate purpose and to limit the risk of criminalizing non-exploitive conduct of children, an unduly expanded range of prohibited content, and the creation, possession or sharing of prohibited content in non-exploitive circumstances [due to a lack of context]. [21-27]

21. Child sexual exploitation and the spread of child sexual abuse material (CSAM) are cyber-enabled offences that engage multiple, complex human rights issues. For these reasons, a cybercrime treaty is not the right forum to discuss them. Human Rights Watch and ARTICLE 19 urge States to uphold their obligations under international human rights law by adopting comprehensive approaches to addressing CSAM.

22. As drafted, Articles 13 and 14 risk infringing on children's rights and criminalizing content that may have scientific, educational, artistic, or literary value. These articles may also restrict the legitimate experience and expression of gender and sexuality of children, including adolescents.[25] Human Rights Watch and ARTICLE 19 are particularly concerned about how criminalizing vaguely defined online content and activity will impact children seeking information about sexual and reproductive health and rights, sexual and gender diversity, discrimination and gender-based violence, and other topics that fall under the rubric of comprehensive sexuality education.

23. States already have international treaty obligations to protect children from sexual exploitation and eradicate the spread of CSAM.[26] 176 States are already parties to the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, which provides for mutual investigative assistance. Human Rights Watch and ARTICLE 19 urge States to uphold their international treaty obligations to

[24] Office of the High Commissioner for Human Rights, "Key-messages relating to a comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes," January 17, 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf, (accessed August 20, 2023); Office of the High Commissioner for Human Rights, *Third Intersessional Consultation*, November 3-4, 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_1_OHCHR.pdf (accessed August 20, 2023): "as experience has shown, if treaty provisions are not precisely drafted, in line with human rights requirements, it opens the door for an implementation into national law that goes beyond what's acceptable from a human rights perspective."

[25] See, for example, UN Committee on the Rights of the Child, General Comment No. 20, The implementation of the rights of the child during adolescence, CRC/C/GC/20, (2016) https://undocs.org/en/CRC/C/GC/20, (accessed August 20, 2023), para. 40: "States should avoid criminalizing adolescents of similar ages for factually consensual and non-exploitative sexual activity."

[26] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OP-CRC-AC), adopted May 25, 2000, G.A. Res. 54/263, Annex II, 54, U.N. GOAR Supp. (No. 49A) at 6, U.N. Doc. A/45/49, Vol. III (2000), entered into force January 18, 2002, https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx (accessed July 17, 2023); See also Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989) entered into force September 2, 1990, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed July 17, 2023), art. 19.

protect children from sexual exploitation and eradicate the spread of CSAM and question whether a cybercrime treaty is a necessary place to impose additional obligations.

24. Human Rights Watch and ARTICLE 19 recommend deleting Articles 13 and14 in their entirety. At the very minimum, the text of these articles should be amended to address the concerns outlined below.[27]

    a. If Article 13 is not deleted in its entirety, we recommend the following amendment to mitigate the risk of criminalizing protected speech:

    > Article 13(2) *bis:* No person shall be convicted of an offence under this article if the act that is alleged to constitute the offence:
    >
    > (a) has a legitimate purpose related to the administration of justice or to science, medicine, education, or art; and
    >
    > (b) does not pose an undue risk of harm to a child.

    b. The term "possession" in Article 13(1)(c) has posed a risk of over-criminalization in many CSAM provisions in national law. Given the nature of computing systems, possession can occur without the knowledge of an individual if, for example, images are shared without solicitation in a general-purpose chat group or images are cached on an individual's local device without their knowledge or awareness.

    The inclusion of "controlling" and "facilitating" in 13(1)(c) and (d), respectively, could also lead to criminal liability for service providers acting as mere conduits. To avoid the risk of prosecution under this clause, intermediaries or controllers may implement preventative measures, like general monitoring of users or device-side scanning, which are disproportionate and undermine the human rights to freedom of expression and privacy.[28] We recommend amending Article 13(1)(c) to read "Knowingly ~~P~~possessing ~~or~~and controlling" and Article 13(1)(d) to read "Financing~~, facilitating~~ or profiting." Article 13 should also be amended to add "13(1*bis):* Nothing in this Article requires a service provider to monitor its services or affirmatively seek facts indicating infringing conduct."

    c. Leaving the terms "sexual activity", "sexual pose", and "sexual purposes" in Article 13(2)(a)(i), (ii), and (iii) undefined in the definition of "child sexual abuse or child sexual exploitation material" risks potentially exceedingly broad application and could result in the criminalization of protected speech.

    The use of "sexual activity or pose" and "sexual activity" in Article 13(2)(a) problematically broadens the scope of criminalized activities. Core international instruments addressing CSAM are limited to

[27] While Article 13(1) is limited to conduct that is "without right" this term, as discussed above, is not sufficiently precise to require exclusion of legitimate activity. It is left to the discretion of States whether to exclude attempts by survivors to report CSAM activity to law enforcement or platforms, documentation or trend analysis of CSAM distribution chains, preservation of evidence by platforms, and other activity. There should be no latitude in this provision for State Parties to, for example, weaponize this provision in order to persecute LGBT survivors who are attempting to document and report their own abuse. Finally, the "without right" exception grants State Parties too much latitude when pursuing their own respective objectives, allowing government agencies, for example, to repurpose CSAM image repositories in order to test facial recognition systems without consent. See Os Keyes, Nikki Stevens, and Jacqueline Wernimont, "The Government is Using the Most Vulnerable People to Test Facial Recognition Software," *Slate*, March 17, 2019, https://slate.com/technology/2019/03/facial-recognition-nist-verification-testing-data-sets-children-immigrants-consent.html (accessed August 20, 2023).

[28] "Explanatory Report to the Convention on Cybercrime," ETS No. 185, November 23, 2001, https://rm.coe.int/16800cce5b (accessed August 20, 2023), para. 105: "This article lists different types of illicit acts related to child pornography which, as in articles 2 – 8, Parties are obligated to criminalise if committed "intentionally." Under this standard, a person is not liable unless he has an intent to offer, make available, distribute, transmit, produce or possess child pornography. Parties may adopt a more specific standard (see, for example, applicable European Community law in relation to service provider liability), in which case that standard would govern. For example, liability may be imposed if there is "knowledge and control" over the information which is transmitted or stored. It is not sufficient, for example, that a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability."

criminalizing "explicit sexual activity" whereas "sexual activity" as a relative term is broader in scope.[29] This is particularly problematic as some jurisdictions define "sexual activity" broadly to include, for example, kissing of a child or even potentially kissing in the presence of a child.[30] Combined with other elements of Article 13, which criminalizes any material that "depicts or represents a child or a person appearing to be a child" engaging in "real or simulated" sexual activity or "in the presence" of sexual activity, this definition could criminalize many artistic, scientific, educational, or literary works that entail no exploitation of children and have no connection to the underlying harm intended to be addressed. Article 13 should not heighten the risk of capturing activity that is not graphic or explicit, such as kissing, by expanding the definition of CSAM in existing core international instruments. We would also suggest that the drafters consider adopting a closed definition of the activity being criminalized in the text of the Proposed Convention.[31]

The vagueness of these terms could result in criminalizing legitimate content under the following circumstances: parents sending photos of a child's sexual organs to a doctor ahead of a consult or as part of a telehealth appointment, adolescents who are above the age of consent but defined as children under this Proposed Convention sharing content of a sexual nature consensually, children seeking access to sexual and reproductive health information, or even family capturing photos of intimate, private moments, photos that when stripped of context could be interpreted as falling under the broad definition of CSAM.[32]

d. Article 13(2)(b) defines "material" to include not only "images" but also "written material." It is not clear the limits of what written material include, and whether this could give rise to the banning or sale of books. Note, for instance, that there exist world-wide best-selling novels (such as the Song of Ice and Fire series by George R.R. Martin, famously adapted to the Game of Thrones television series) that frequently describe or depict brutal acts as part of their story, including sexual abuse of children.[33] Far from fringe works, these novels have been translated into 47 languages, sold nearly 100 million copies worldwide, and adapted into one of the most popular television series globally of all time.[34] Part of the appeal of the stories for many is the grim social commentary they provide on war and history. Nevertheless, criminalizing the possession or sale of this book would appear to be encouraged by Article 13, as drafted.

   The Draft Text appears to address this by offering optional protections for expression in Article 13(3), allowing States to limit laws to instances featuring a real child or visual depictions. We are concerned that given the discretionary nature, this section does not provide a strong enough protection against infringements on artistic or literary expression.

---

[29] OP-CRC-AC, art 2(c); Convention on Cybercrime, ETS No. 185, (2001), entered into force January 7, 2004, https://rm.coe.int/1680081561 (accessed August 20, 2023), art 9(2)(a)-(c). Note also "Explanatory Report to the Convention on Cybercrime," ETS No. 185, November 23, 2001, https://rm.coe.int/16800cce5b, (accessed August 20, 2023, para. 100.

[30] See, for example, discussion at James McNicol and Andreas Schloenhardt, "Australia's Child Sex Tourism Offences," *Current Issues in Criminal Justice*, vol. 23(3) (2012), https://www.austlii.edu.au/au/journals/CICrimJust/2012/5.pdf (accessed August 20, 2023), pp. 380-382; "Age of Consent to Sexual Activity," Government of Canada, Department of Justice, accessed August 20, 2023, https://justice.gc.ca/eng/rp-pr/other-autre/clp/faq.html.

[31] A closed definition could build on: "Explanatory Report to the Convention on Cybercrime," ETS No. 185, November 23, 2001, https://rm.coe.int/16800cce5b (accessed August 20, 2023), para. 100.

[32] Kashmir Hill, "A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal," *New York Times*, August 21, 2022, https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html (accessed August 20, 2023).

[33] "Rape in ASOIAF vs. Game of Thrones: a statistical analysis," post to Tumblr, 24 May 2015 (warning: graphic written descriptions) https://tafkarfanfic.tumblr.com/post/119770640640/rape-in-asoiaf-vs-game-of-thrones-a-statistical (accessed August 24, 2023).

[34] Robin Dunbar, "Science reveals secrets behind the success of Game of Thrones," *Oxford News Blog*, November 3, 2020, https://www.ox.ac.uk/news/arts-blog/science-reveals-secrets-behind-success-game-thrones (accessed August 24, 2023).

e. Article 13(4) takes steps to decriminalize the creation of sexual material by children but does not go far enough to protect children's free expression when it comes to sharing of consensual material between them (self-generated or not). The Committee on the Rights of the Child has advised that "States should avoid criminalizing adolescents of similar ages for factually consensual and non-exploitative sexual activity."[35] Requiring that States Parties "take steps" is not sufficient to protect children who are above the age of consent but still defined as children for the purposes of this Proposed Convention from being prosecuted for self-generated material. The focus on self-generation is both too narrow in some contexts and too broad in others. For example, it does nothing to protect partners who consensually *possess* such material or the consensual sharing of material that is not self-generated. But it also fails to criminalize material that a child is coerced into creating, which is technically captured by them on their own device and could be considered self-generated.

Recommendation 5: Delete Article 14 in its entirety. If the provision is nonetheless retained, amend Article 14 to limit the risk of criminalizing activities of children who are above the age of consent but still captured by the Draft Text, of criminalizing people seeking or imparting information regarding sexual and reproductive health, and of the use of these provisions to discriminate against same-sex interactions. [25-27]

25. "Solicitation for sexual purposes" under Article 14 is too vague, and could potentially criminalize sexual acts, or even just communicating about sexual acts with children who are above the age of consent but still defined as children for the purposes of this Proposed Convention. "Communicating" or "making any arrangement with a child for sexual purposes" could include communications about sexual and reproductive health information, like obtaining contraceptives or even just learning about them, obtaining information about one's own body, and finding community or counseling for LGBT and other children International human rights law guarantees children a right to information about sexual and reproductive health, yet efforts to provide adequate sexual and reproductive health information frequently face a concerning backlash.[36] The term "solicitation" may also be problematic as it is appears in national cybercrime legal provisions that have been used to target LGBT people.[37]

26. The issues we highlight in relation to Articles 13 and 14 above are compounded in jurisdictions where there has already been a push to criminalize pornography. For example, regional instruments such as the Arab Convention on Cybercrime broadly call for punishment of pornography; where this is the case, terminology like "sexual activity" may be interpreted broadly to target material that is protected under international human rights law.

27. These terms could also be interpreted to discriminate against same-sex interactions, which have historically been targeted under obscenity, "morality," indecency, and pornography laws. Human Rights Watch and ARTICLE 19 have documented that cybercrime laws, sometimes used in conjunction with laws criminalizing consensual same-sex conduct, "inciting debauchery," "debauchery," and "prostitution," are used to target and prosecute LGBT people, regardless of whether same-sex acts occur, creating a climate in which LGBT people can be

[35] UN Committee on the Rights of the Child, General Comment No. 20, The implementation of the rights of the child during adolescence, CRC/C/GC/20 (2016), https://undocs.org/en/CRC/C/GC/20 (accessed August 20, 2023), para. 40.

[36] "Submission to the UN Special Rapporteur on the Right to Privacy," Human Rights Watch submission, October 19, 2020, https://www.hrw.org/news/2020/10/19/submission-human-rights-watch-un-special-rapporteur-right-privacy, paras. 16-20.

[37] Human Rights Watch, *"All This Terror Because of a Photo": Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa* (New York: Human Rights Watch, 2023), https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt. For negative impact of CSAM offences on LGBT people beyond the MENA region See Derechos Digitales, "When protection becomes threat: Cybercrime regulation as a tool for silencing women and LGBTQIA+ people around the world," June 20, 2023, https://www.apc.org/en/node/38844/ (accessed August 20, 2023); and ARTICLE 19 et al, "Letter to INHOPE," January 20, 2020, https://www.article19.org/resources/inhope-members-reporting-artwork-as-child-sexual-abuse/ (accessed August 20, 2023).

prosecuted merely for expressing themselves online, in particular in Middle East and North African countries.[38] A significant study of the role of digital evidence in the persecution of LGBT people in Egypt, Lebanon, and Tunisia found that due to increased reliance on digital evidence as a component of prosecution, there is a corresponding increase in the use of cybercrime laws to persecute LGBT people.[39]

Article 15: Avoid infringing on the rights of survivors of online gender-based violence

Recommendation 6: Consider the appropriateness of including Article 15. If the provision is retained, amend Article 15 to mitigate the risk of criminalizing survivors particularly where the perpetrator is an authority figure, to center the lack of freely given consent, to criminalize the non-consensual capturing of intimate images and to exempt conduct that is a matter of public interest or for a legitimate purpose related to the administration of justice. [28-31]

28. The non-consensual dissemination of intimate images (NCDII) is a form of gender-based violence. It engages multiple, complex human rights issues and for these reasons, a cybercrime treaty is not the right forum to discuss them. Under the Convention on the Elimination of Discrimination against Women (CEDAW), States have a responsibility to protect the right to live free from gender-based violence, including in online and virtual spaces, and outline state obligations to fulfill that right.[40] CEDAW and other treaties require States to show due diligence in preventing violation of rights by private actors and to investigate and punish acts of violence.[41]

29. As drafted, Article 15 falls short by potentially encroaching on women's rights, in particular the rights of survivors. For example, Article 15(1) could be used against survivors, especially if the perpetrator is an authority figure. For example, if a survivor has documented abuse of a sexual nature, transmitting evidence of such abuse in an effort to gain access to justice could be criminalized with this clause. Criminalizing acts cannot be justified if their purpose or effect is to prevent legitimate criticism of public figures, the exposure of corruption, official wrongdoing, or to protect the reputation of heads of state or other public officials or public figures.[42]

30. Likewise, Article 15(2), which defines "intimate image" is drafted too broadly and could include artistic expression and satire as forms of "representation." Additionally, "reasonable expectation of privacy" is not a commonly understood standard in international human rights law and its use here without context does not provide sufficient clarity to delineate the scope of this criminal provision.[43]

31. Article 15 should be revised to focus on the lack of freely given consent. It should also include an exception for matters of public interest to avoid the use of privacy claims to interfere with the administration of justice for

---

[38] Human Rights Watch, *"All This Terror Because of a Photo": Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa* (New York: Human Rights Watch, 2023), https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt.

[39] Afsaneh Rigot, "Digital Crime Scenes," Berkman Klein Center, March 7, 2022, https://cyber.harvard.edu/publication/2022/digital-crime-scenes (accessed July 24, 2023).

[40] Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), adopted December 18, 1979, G.A. res. 34/180, 34 U.N. GAOR Supp. (No. 46) at 193, U.N. Doc. A/34/46, entered into force September 3, 1981, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women (accessed August 20, 2023). UN General Assembly, "Intensifying global efforts for the elimination of female genital mutilation," Resolution 71/168, A/RES/71/168, https://undocs.org/en/A/RES/71/168 (accessed August 20, 2023); UN Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet," Resolution 32/13, A/HRC/RES/32/13, https://undocs.org/en/A/HRC/RES/32/13 (accessed August 20, 2023).

[41] CEDAW, art. 2(3); UN Committee on the Elimination of Discrimination against Women, General Comment No. 35, Gender-based Violence Against Women, CEDAW/C/GC/35, July 26, 2017, https://undocs.org/en/CEDAW/C/GC/35 (accessed August 20, 2023).

[42] ARTICLE 19, "The Global Principles on Protection of Freedom of Expression and Privacy, March 2017, https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf, (accessed August 20, 2023), Principles 3 and 13.

[43] *R v. Jarvis*, Supreme Court of Canada, 1 SCR 488, Judgment, February, 14, 2019, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/17515/index.do (accessed August 24, 2023), paras. 54-56; Criminal Code, RSC 1985, c C-46, ss. 162.1(2)(c).

gender-based violence or without justification in order to prevent the dissemination of information about matters in which the public has an interest or concern of being informed;[44]

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the **recording**, offering, selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of [a computer system] [an information and communications technology device], without the **freely given** consent of the person depicted in the image.
2. For the purpose of paragraph 1, "intimate image" shall mean a visual recording or representation of a natural person made by any means, including a photograph, film or video recording in which the person is nude, is exposing their genital organs, anal region or breasts, or is engaged in **explicit** sexual activity, and in respect of which, **there was an absence of freely given consent** at the time of the recording **or dissemination** ~~there were circumstances that gave rise to a reasonable expectation of privacy~~.

Article 15(2)*bis:* No person shall be convicted of an offence under this article if the act that is alleged to constitute the offence has a legitimate purpose related to the administration of justice or a matter of the public interest;

Articles 6-10: Core cybercrime provisions lack key safeguards and limitations

Recommendation 7: Amend Articles 6-10 so that: fraudulent or otherwise malicious intent conduct must result in serious harm or damage in order to be criminalized, bypassing technical safeguards is a core element of each criminal act, and a public interest exception is included. [32-33]

Article 10bis. Limitations and Public interest exception

1. Articles 6-10 shall not apply to any person who uses or discloses information for the purpose of revealing a misconduct, wrongdoing, fraud, an illegal activity or a human rights violation or where a person acted in the public interest or for the purpose of protecting a general public interest.

2. A State Party shall require that the conduct described in paragraphs 1 of Articles 6 to 10 result in serious harm and that the offences in Articles 6 to 10 be committed by infringing security measures and with fraudulent or otherwise malicious intent.

32. The core cybercrime offences contained in Articles 6-10 are drafted in such a way that they risk criminalizing legitimate activities, especially those carried out by journalists, human rights defenders, and security researchers. We recommend consolidating the following safeguards and restrictions in Article 10*bis* and amending Articles 6 to 10 accordingly:

- The requirement that the acts committed in these Articles be "committed intentionally" should be retained and clarified to specify that the **intent should be fraudulent or otherwise malicious**[45] to avoid criminalizing very common practices, such as the sharing of passwords for online services among family and friends, or routine work of independent security researchers and whistleblowers, which could chill crucial cybersecurity work and access to public interest information.[46]

[44] ARTICLE 19, "Global Principles on Protection of Freedom of Expression and Privacy," March 2017, https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf (accessed August 20, 2023): defines "public interest" as encompassing "matters in which the public has an interest or concern of being informed. This includes, but is by no means limited to, information about matters that affect the functioning of the state, public officials and public figures, politics, public health and safety, law enforcement and the administration of justice, the protection of human rights, consumer and social interests, the environment, economic issues, the exercise of power, art and culture, or matters that affect general interests or entail major consequences."

[45] Note that the Budapest Convention and Article 6 of the Draft Text use the term "dishonest intent" to signify the same intent requirement and provides examples of its scope. See, for example, "Explanatory Report to the Convention on Cybercrime," ETS No, 185, November 23, 2001, https://rm.coe.int/16800cce5b (accessed August 20, 2023), para. 90.

[46] *United States v Nosal*, United States Court of Appeals for the Ninth Circuit, 828 F.3d 865 (2016), https://casetext.com/case/united-states-v-nosal-28 (accessed August 20, 2023).

- Articles 6-10 should be strengthened by adding a requirement that they **result in serious harm or damage**, to avoid far-reaching criminalization as well as far- reaching procedural and law enforcement measures, beyond what is necessary and proportionate.
- Articles 6 and 8-10 should explicitly require the **bypassing of technical safeguards** as a core element of the criminal act. Absent this requirement, the risk of criminal sanctions on the basis of terms of use violations is too great and could allow service providers to unilaterally establish the scope of criminal liability.[47]
- A **public interest exception** should be added to ensure that the treaty cannot be instrumentalized to restrict the legitimate work of civil society organizations, journalists, security researchers, whistle-blowers and other actors pursuing the public interest.

33. The Draft Text currently relies on a "without right" qualifier that is too undefined and permissive a concept to address the specific and well documented negative impacts core cybercrime offences can have. Over two decades of experience has demonstrated that these activities are not sufficiently excluded through a "without right" qualifier and Articles 6-10 instead require specific limitations. The term is widely used in the Budapest convention to prevent overcriminalization in light of the broad range of conduct covered by these offences The concept of "without right" is best suited to shielding activities approved by service providers but not where service providers are incentivized to withhold authorization by contractual or other means because their interests are at odds with other individuals.[48] The ambiguity places too powerful a tool in the hands of prosecutors, who have threatened individuals with severe criminal penalties for what are at best minor infractions.[49] National courts have struggled to prevent cybercrime provisions from over-criminalizing activity that does not constitute "hacking" or bypassing technical safeguards to access a computer system. Service providers and employers have been empowered to prohibit pro-consumer interoperability content scraping tools,[50] stifle legitimate security research and tools,[51] prevent legitimate users of a system or service from authorizing others to access it including through password sharing,[52] and criminalize government or corporate whistleblowers.[53]

---

[47] Peter G Berris, "Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress," Congressional Research Service, September 21, 2020, https://crsreports.congress.gov/product/pdf/R/R46536 (accessed August 20, 2023), pp. 24-26.

[48] "Explanatory Report to the Convention on Cybercrime," ETS No, 185, November 23, 2001, https://rm.coe.int/16800cce5b (accessed August 20, 2023), para. 38.

[49] Jamie Williams, "New Federal Guidelines for Computer Crime Law Do Nothing to Reign in Prosecutorial Overreach Under Notoriously Vague Statute", Electronic Frontier Foundation, October 31, 2016, https://www.eff.org/deeplinks/2016/10/what-were-scared-about-halloween-prosecutorial-discretion-under-notoriously-vague (accessed August 20, 2023); Marcia Hoffman, "In the Wake of Aaron Swartz's Death, Let's Fix Draconian Computer Crime Law," Electronic Frontier Foundation, January 14, 2013, https://www.eff.org/deeplinks/2013/01/aaron-swartz-fix-draconian-computer-crime-law (accessed August 20, 2023); Katitza Rodriguez and Aaron Mackey, "Dear Canada: Accessing Publicly Available Information on the Internet is Not a Crime," Electronic Frontier Foundation, April 19, 2018, https://www.eff.org/deeplinks/2018/04/dear-canada-accessing-publicly-available-information-internet-not-crime (accessed August 20, 2023); Cindy Cohn, "Raid on COVID Whistleblower in Florida Shows the Need to Reform Overbroad Computer Crime Laws and the Risks of Over-Reliance on IP Addresses," Electronic Frontier Foundation, December 10, 2020, https://www.eff.org/deeplinks/2020/12/raid-covid-whistleblower-florida-shows-need-reform-overbroad-computer-crime-laws (accessed August 20, 2023); Amie Stepanovich, "Testimony Before the Advisory Committee on Criminal Rules on the Matter of Proposed Amendments to the Federal Rules of Criminal Procedure, Rule 41," Access Now, https://www.accessnow.org/wp-content/uploads/archive/docs/Rule41botnettestimony.pdf (accessed August 20, 2023).

[50] *Facebook v. Power Ventures*, United States Court of Appeals for the Ninth Circuit, 844 F.3d 1058, Amended Decision, September 12, 2016 https://www.eff.org/files/2016/12/14/facebook_v._power_ventures_-_amended_decision.pdf (accessed August 20, 2023).

[51] Nate Cardozo, Kurt Opsahl, Katitza Rodriguez, Ramiro Ugarte and Jamie Lee Williams, "Protecting Security Researchers' Rights in the Americas," Electronic Frontier Foundation, September 2018, https://www.eff.org/files/2018/10/09/protecting_security_researchers_rights_in_the_americas-eff.pdf (accessed August 20, 2023).

[52] *United States v. Nosal*, United States Court of Appeals for the Ninth Circuit, 828 F.3d 865 (2016), https://casetext.com/case/united-states-v-nosal-28 (accessed August 20, 2023).

[53] See Brief for the National Whistleblower Center, *Amicus Curiae*, in *Van Buren v. United States*, Supreme Court of the United States, File No 19-783, https://www.supremecourt.gov/DocketPDF/19/19-783/147217/20200708130837153_NWC%20Main%20Document.pdf (accessed August 20, 2023); Bill Chappell and Rachel Treisman, "Data Scientist Rebekah Jones, Facing Arrest, Turns Herself in to Florida Authorities," *NPR*, January 18, 2021, https://www.npr.org/sections/coronavirus-live-updates/2021/01/18/957914495/data-scientist-rebekah-jones-facing-arrest-turns-herself-in-to-florida-authoriti (accessed August 20, 2023); April Boyer, Jonathan B Morton and Rio J Gonzalez, "SCOTUS Resolves Circuit

Draft Text's overall human rights provisions fall short

34. The lack of adequate human rights safeguards is particularly concerning in light of the nature and scope of this convention. In contrast to other criminal law instruments overseen by the United Nations Office of Drugs and Crime (UNODC), cybercrime offences have been abused to attack human rights defenders, journalists, whistleblowers, and political dissidents.[54] Contrary to other UNODC instruments, the Draft Text's scope is expansive and currently includes policing measures in relation to any serious crime.

Paragraphs 9, 11 and 12 of the preamble & Article 5

> **Recommendation 8: Amend Article 5 so that it ensures the Proposed Convention does not threaten human rights and to mainstream a gender perspective and take into consideration the circumstances of persons and groups who face discrimination and marginalization, amend the preamble to add Paragraph 9*bis* recognizing the important role of civil society, the Office of the High Commissioner for Human Rights and the international human rights mechanisms in the implementation of the Proposed Convention, and amend Paragraphs 11 and 12 of the preamble so that international human rights law and standards are reflected. [35-38]**

35. The Draft Text introduces state obligations that are likely to have a profound impact on human rights. We propose amendments to Article 5 to articulate the human rights protections that are required to ensure that nothing in the Proposed Convention threatens human rights, most notably rights to privacy, freedom of expression, and due process, and to in particular safeguard the rights of persons and groups in positions of vulnerability and marginalization who are more likely to have their rights violated both by cybercrime and by efforts to address it. We propose the following amendments to Article 5:

> *Article 5. Respect for human rights*
>
> 1. States Parties shall carry out ~~ensure that the implementation of~~ their obligations under this Convention ~~is consistent with their obligations~~ in accordance with international human rights law, including but not limited to rights arising pursuant to their obligations under the International Covenant on Civil and Political Rights, the Convention on the Rights of the Child, Convention on the Elimination of All Forms of Discrimination against Women, the International Covenant on Economic, Social, and Cultural Rights, and additional protocols and other applicable international human rights instruments, and which shall incorporate the principles of legality, necessity and proportionality.
>
> 2. States Parties shall
>
> (a) mainstream a gender perspective and to empower women and girls, and shall
>
> (b) take into consideration the special circumstances and needs of persons and groups who face discrimination and marginalization in measures undertaken to prevent and combat [the use of information and communications technologies for criminal purposes] [cybercrime].

36. Elements of the preamble that seek to address human rights also fail to provide sufficient context to ensure the Proposed Convention will respect human rights in its adoption and implementation.[55] We propose Paragraph 9b*is*,

Split, Limits Scope of the Computer Fraud and Abuse Act," *National Law Review*, vol. 13 (209) (2023), https://www.natlawreview.com/article/scotus-resolves-circuit-split-limits-scope-computer-fraud-and-abuse-act (accessed August 20, 2023).

[54] Summer Walker, "Still Poles Apart: UN Cybercrime Treaty Negotiations," June 2023, Global Initiative Against Transnational Organized Crime, https://globalinitiative.net/wp-content/uploads/2023/06/Summer-Walker-Poles-apart-UN-cybercrime-treaty-negotiations-GI-TOC-June-2023.pdf, (accessed August 20, 2023), pp. 5-6.

[55] Office of the High Commissioner for Human Rights, "Key-messages relating to a comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes," January 17, 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf, (accessed August 20, 2023); Ad Hoc

recognizing that civil society, the Office of the High Commissioner for Human Rights, and the international human rights mechanisms will play a key role in ensuring that implementation of the treaty is human rights compliant:

> 9*bis* Recognizing the role and participation of civil society, the Office of the High Commissioner for Human Rights and the international human rights mechanisms as key to ensuring that the implementation of this Convention is human rights compliant.

37. Paragraph 11 should be amended as follows to ensure that clarify the applicability of international human rights law and standards:

> *(11) Mindful* of the need to achieve law enforcement objectives and to ensure respect for human rights and fundamental freedoms as enshrined in applicable international and regional instruments, and international human rights law and standards,

38. Paragraph 12 of the preamble acknowledges the right to protection against unlawful interference with the right to privacy, including the protection of personal data. The provision undermines the right to privacy by limiting its scope of recognition to "unlawful" interferences, meaning it only recognizes interferences with privacy that are not provided for under law. This amounts to a misrepresentation of international human rights law, which requires that any interference with the right to privacy including with the right to data protection cannot be unlawful or arbitrary and that it must comply with the principles of legality, necessity, and proportionality.[56] The text of Paragraph 12 should be amended to reflect this:

> *(12)* ~~*Acknowledging* the right to protection against unlawful~~ *Stressing* that any interference with the right to privacy, including the right to personal data protection ~~of personal data~~, should comply international human rights law, which shall at a minimum incorporate the principles of legality, necessity, and proportionality

General safeguard in Articles 21, 23, 24 and 35 require more robust protections for human rights.

> **Recommendation 9: Amend Articles 21, 23, 24 and 35 to align the Draft Text's core safeguards regarding due process, investigative powers and international cooperation with international human rights law including through incorporation of the principles of legality, necessity, proportionality, and dual criminality. [39-43]**

39. The Draft Text's core safeguards, Articles 21, 23, 24 and 35, fall short of requirements in international human rights law.

Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes Third Intersessional Consultation, "Statement of the Office of the High Commissioner for Human Rights," November 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_1_OHCHR.pdf (accessed August 20, 2023): "as experience has shown, if treaty provisions are not precisely drafted, in line with human rights requirements, it opens the door for an implementation into national law that goes beyond what's acceptable from a human rights perspective."

[56] For a compendium of relevant international and regional human rights standards, resolutions, and jurisprudence, see Privacy International, "Guide to International Law and Surveillance," January 31, 2022, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance (accessed August 20, 2023). See also UN Human Rights Committee, "Concluding observations on the fourth periodic report of the United States of America," CCPR/C/USA/CO/4, April 23, 2014, https://undocs.org/en/CCPR/C/USA/CO/4 (accessed August 20, 2023), para. 22(a): "…measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity…"; UN General Assembly, Report of the United Nations Special Rapporteur on the right to privacy, A/77/196, July 20, 2022, https://undocs.org/en/A/77/196 (accessed August 20, 2023), paras. 1-11.

40. Article 21 does not reflect the principle that criminal sanction should only be reserved for the most serious conduct[57] and falls short of requiring reasonable doubt as a condition of conviction as well as compliance with the principles of legality, necessity and proportionality.[58] We would recommend the following amendments:

> 21(3) Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences established in accordance with articles 6 to 16 of this Convention are exercised in order to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences **and to promote environments conducive to non-offending and rehabilitation of offenders**.
>
> 4. Each State Party shall ensure that any person prosecuted for offences established in accordance with articles 6 to 16 of this Convention enjoys all rights and guarantees in conformity with domestic law and consistent with ~~the obligations of the State Party under~~ international human rights law, including the right to a fair trial**, the right to the presumption of innocence,** and the rights of defence **and incorporating the principles of legality, strict necessity and proportionality**.

41. Article 23 is no longer limited in scope to measures established for the purpose of specific criminal investigations and proceedings, opening the door to mass, bulk or indiscriminate surveillance by removing the obligation to ensure investigative powers are used in connection with individual cases concerning particular suspects.[59] We are concerned that this important limiter, which was present in previous drafts of this provision, has been removed and recommend its reinstatement:

> 23(1) Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of **specific** criminal investigations or proceedings.

42. Article 24 fails to incorporate the principles of necessity and legality and the need for prior judicial authorization premised on a robust factual basis prior to any interference with the right to privacy, including the right to data protection.[60] Accordingly we recommend the following amendments:

> 24(1). Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards ~~provided for under~~ **defined by** its domestic law, which shall be **in compliance with** ~~consistent with its~~

---

[57] UN General Assembly Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, Discussion Guide, A/CONF.222/PM.1, July 19, 2013, https://undocs.org/en/A/CONF.222/PM.1 (accessed August 20, 2023), paras. 47(e) and 80.

[58] UN Human Rights Committee, General Comment No. 35, Liberty and Security of Person, CCPR/C/GC/35 (2014), https://undocs.org/en/CCPR/C/GC/35 (accessed August 20, 2023), paras. 12, 22-25 and 33-35: "An arrest or detention…must be interpreted…to include elements of inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity and proportionality."); UN Human Rights Committee, General Comment No.32, Right to equality before courts and tribunals and to a fair trial, CCPR/C/GC/32, August 23, 2007, https://undocs.org/en/CCPR/C/GC/32 (accessed August 20, 2023), para. 30; "The presumption of innocence, which is fundamental to the protection of human rights, imposes on the prosecution the burden of proving the charge, guarantees that no guilt can be presumed until the charge has been proved beyond reasonable doubt, ensures that the accused has the benefit of doubt, and requires that persons accused of a criminal act must be treated in accordance with this principle."

[59] Convention on Cybercrime, ETS No. 185, November 23, 2001, https://rm.coe.int/1680081561 (accessed August 20, 2023), art 14(1); Explanatory Report to the Convention on Cybercrime, ETS No. 185, November 23, 2001, https://rm.coe.int/16800cce5b (accessed August 20, 2023), paras. 135, 152 and 181-182: "As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorize Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining." We note also that decisions allowing interference with the right to privacy must be made on a case-by-case basis: UN Human Rights Committee, *Lula da Silva v Brazil*, CCPR/C/134/D/2841/2016, May 24, 2022, https://undocs.org/en/CCPR/C/134/D/2841/2016%20(FINAL%20PROCEEDINGS) (accessed August 20, 2023), para. 8.7; UN Human Rights Committee, General Comment No 16, The Right to Privacy, (1988), https://www.refworld.org/docid/453883f922.html (accessed August 24, 2023), para. 8.

[60] Privacy International and Electronic Frontier Foundation, "Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V & VII," July 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Privacy_Intl_EFF.pdf (accessed August 20, 2023), pp. 3-5.

~~obligations under~~ international human rights law, ~~and which shall~~ incorporating at a minimum ~~incorporate~~ the principles of legality, necessity, and proportionality, and require a factual basis justifying the use of such powers and procedures.

2. Such conditions and safeguards shall, ~~as appropriate in view of the nature of the procedure or power concerned~~, inter alia, include prior judicial or other independent authorization and review, demonstrable grounds justifying application, and limitation of the scope and the duration of such power or procedure, publication of statistical information periodically detailing the use of powers and procedures, remedial actions taken, adequate notification and access to effective remedies, and reasonable retention limitations.

43. Article 35 establishes general principles for international cooperation. These principles exclude critical limitations and safeguards adopted elsewhere in the Draft Text and require no dual criminality condition.[61] Absent these safeguards and limitations, Article 35 creates a framework for international cooperation that threatens human rights.[62] We recommend the following amendments to address these limitations:

35(1) States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of specific investigations, prosecutions and judicial proceedings concerning offences established in accordance with articles 6 to 16 of this Convention…

1bis. Cooperation between State Parties shall be in compliance with international human rights law, incorporating at a minimum the principles of legality, necessity, and proportionality, shall respect the principle of dual criminality, and shall occur only where resulting prosecutions shall be in compliance with international human rights law, including the right to a fair trial, the right to the presumption of innocence, and the rights of defense.

2. In matters of international cooperation, ~~whenever~~ the principle of dual criminality ~~is~~ shall be ~~considered~~ a requirement, and ~~it~~ shall be deemed fulfilled irrespective of whether the laws…

Scope and Breadth of the Draft Text's policing and cooperation powers

44. The Draft Text's policing and international cooperation measures continue to apply well beyond offences set out in Articles 6 – 10 of the Draft Text. In addition, a number of the Draft Text's specific policing and cooperation powers are too broad and threaten to infringe on human rights.

Chapters IV-V: Limit scope of policing powers and cooperation to offences established in the Convention

Recommendation 10: Delete Articles 23(2)(b) and 23(2)(c), and amend Articles 35(1), 40(1), 40(4), 41(1), 45(2), 47(1) and 47(1)(b)(if retained) so that international cooperation and mutual legal assistance are limited to in scope to offences established in accordance with Articles 6 to 16 of the Draft Text. [45-50]

- Provisions in Article 23(2)(b) and 23(2)(c), extending the scope of the Draft Text's procedural measures beyond offences set out in Articles 6 to 16 should be stricken entirely.
- Article 35(1) outlining the general scope of international cooperation should be amended so that international cooperation obligations do not apply to the collection, obtaining, preservation and sharing

[61] Article 21 (due process) is limited in application to offences set out in Article 6 to 16 of the Draft Text. Article 24 (conditions and safeguards) only applies to measures adopted in accordance with Chapter IV.

[62] Privacy International and Electronic Frontier Foundation, "Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V & VII," July 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Privacy_Intl_EFF.pdf (accessed August 20, 2023), pp. 7-8.

of evidence in electronic form of "serious crimes, including offences covered by article 17 of this Convention when applicable."

- Article 40(1) outlining the scope of mutual legal assistance requirements should be amended so that mutual legal assistance for the purposes of collecting evidence in electronic forms does not apply to "serious crimes, including offences covered by article 17 of this Convention when applicable."
- Article 40(4) authorizing State Parties to proactively share information should replace "information relating to criminal matters" with "information relevant to specific investigations, prosecutions and judicial proceedings of offences established in accordance with Articles 6 to 16 of this Convention."
- Article 41(1) obligating State Parties to join a 24/7 network should be amended so that it provides no independent authority for immediate assistance unless it is "in accordance with Article 40 of this Convention" and to preclude immediate assistance for the purpose of collecting evidence in electronic form of "serious crime, including those offences covered by article 17 of this Convention when applicable."
- Article 45(2) outlining cooperation on real-time collection of traffic data should amended as follows:

  > 45(2) Each State Party shall provide such assistance ~~at least~~ with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case **and which are established in accordance with Articles 6 to 16 of this Convention**.

- Article 47(1) and 47(1)(b) (if retained) on direct law enforcement cooperation should each replace "offences covered by this Convention" with "specific offences established in accordance with Articles 6 to 16 of this Convention."

45. We appreciate that many elements of Chapters IV-V of the Proposed Convention, which outline a series of investigative and enforcement powers and international cooperation mechanisms, are now properly limited in application to offences established in accordance with Articles 6 to 16 of the Draft Text. By virtue of Article 17, however, many of these otherwise limited provisions are extended in application to numerous other offences and many other provisions in Chapters IV-V continue to apply to all serious offences rather than those explicitly articulated in Articles 6 to 16 of the Draft Text.[63] This ongoing over-reach has the negative effect of diluting expertise and resources that would otherwise be directed to core cybercrime offences, splintering efforts at international cooperation and particularly efforts to address online and physical dimensions of offences adopted in other instruments and included only by virtue of Article 17, and raising concerns over the adequacy of human rights safeguards.[64]

46. Chapter V of the Draft Text in particular provides for increased international cooperation between States Parties for the purpose of investigations, prosecutions and judicial proceedings concerning offences in Articles 6 to 16 and the collection, obtaining, preservation and sharing of evidence in relation to any serious offences. With respect to the gathering of electronic evidence in relation to any serious offences, Chapter V requires State Parties to afford one another the widest measure of mutual legal assistance and to designate a point of contact available 24 hours a day, 7 days a week, in order to ensure the provision of immediate assistance. Extending the scope of mutual legal assistance to all serious offences is deeply problematic in the absence of a dual criminality requirement. States will be obligated to assist on offences established in treaties they have explicitly chosen not to adopt, and on crimes that offend fundamental rights. As the Draft Text's due process obligations are strictly a

63 We note parenthetically that the formulation used in Articles 35(1) and 41(1) to bring offences covered by Article 17 within the scope of the Proposed Convention ("serious crimes, including offences covered by article 17 of this Convention when applicable") could create the unintended problem of rendering any offence adopted by means of Article 17 into a "serious offence."

64 Privacy International and Electronic Frontier Foundation, "Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V & VII," July 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Privacy_Intl_EFF.pdf (accessed August 20, 2023); ARTICLE 19, "Comments on the "Zero Draft" of the UN Cybercrime Convention," July 2023, https://www.article19.org/wp-content/uploads/2023/07/ARTICLE-19-analysis-of-the-Cybercrime-Convention-Zero-Draft-Final.pdf (accessed August 20, 2023).

function of its core criminal provisions,[65] while its human rights safeguards do not apply to its international cooperation provisions,[66] States will also be obligated to cooperate in instances where human rights protections fall short.

47. The extension of some obligations would dilute their effectiveness by compelling cooperation on a wide range of offences rather than on core cybercrimes that would benefit from specific cooperation. Article 47(1)(b), for example, obligates State Parties to cooperate on any offences covered by the Convention without assessing whether this level of mandatory cooperation is necessary or even helpful with respect to all offences included by virtue of Article 17.

48. In many contexts, there is minimal benefit to applying this obligation so broadly and despite an absence of dual criminality, due process obligations, and human rights safeguards. For example, limiting the scope of compelled cooperation in Article 41 to offences set out in Articles 6 to 16 and to cooperation measures specifically articulated in the Convention would preserve the Convention's safeguards and limitations and avoid an obligation to assist in the absence of dual criminality while not precluding State Parties from informal cooperation more broadly. State Parties will join the pre-existing and informal 24/7 cooperation network that has existed since 1990 to fulfill their obligations under Article 41 and so will be well placed to cooperate more broadly, if selectively, once they are members.[67] In addition, the 24/7 network is intended to operate as a window to expedited mutual legal assistance requests.[68] As currently drafted Article 41 authorizes parties to wholly bypass the regime established in Article 40 including the need for a central authority to assess requests against grounds for refusal set out in Article 40(21).[69]

49. In other instances, applying the Proposed Convention's provisions to all serious crimes would create overlapping cooperation mechanisms. The Draft Text provides for this increased international cooperation for any offences without regard to any pre-existing cooperation mechanisms in place regarding those offences. This risks creating multiple and potentially inconsistent or conflicting obligations for international cooperation among States Parties to treaties that would fall under Article 17, as well as potentially inconsistent or conflicting safeguards. As a recent report prepared by the UN Security Council's Counter-Terrorism Committee Executive Directorate noted in the context of international cooperation on lawful access to digital evidence, competing and conflicting mechanisms

65 Article 21 applies to offence established in accordance with Articles 6 to 16, and has no application to offences incorporated into the Draft Text by virtue of Article 17 or because these provisions constitute "serious crimes" under Article 35.

66 Article 24 is limited in application to the "establishment, implementation and application" of powers and procedures provided for in Chapter IV of the Draft Text.

67 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), "The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspective," CTED Trends Report, January 2022, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf (accessed August 20, 2023), pp. 22-23.

68 Explanatory Report to the Convention on Cybercrime, ETS No. 185, November 23, 2001, https://rm.coe.int/16800cce5b (accessed August 20, 2023), para. 301: "among the critical tasks to be carried out by the 24/7 contact is the ability to facilitate the rapid execution of those functions it does not carry out directly itself. For example, if a Party's 24/7 contact is part of a police unit, it must have the ability to co-ordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance, in order that appropriate action may be taken at any hour of the day or night." See also Thomas Dougherty, "G7 24/7 Cybercrime Network," presentation at the International conference organized by the Council of Europe in cooperation with the Information and Communication Agency (ICTA) of Sri Lanka and the Sri Lankan Computer Emergency Readiness Team (SLCERT), https://rm.coe.int/1680303ce2 (accessed August 20, 2023), slide 6: "To use this Network, law enforcement agents seeking assistance from a foreign Participant may contact the 24-hour point of contact in their own state or autonomous law enforcement jurisdiction, and this individual or entity will, if appropriate, contact his or her counterpart in the foreign Participant. Participants in the Network have committed to make their best efforts to ensure that Internet Service Providers freeze the information sought by a requesting Participant as quickly as possible. Participants have further committed to make their best efforts to produce information expeditiously. This is subject to the understanding that a requested Participant's legal, technical or resource considerations may affect the extent to which - and the time frame within which – the Participant may produce evidence, as well as the process of Mutual Legal Assistance, by which the requesting country seeks release of that information though the usual MLAT or Letters of Request procedure."

69 Privacy International and Electronic Frontier Foundation, "Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V & VII," July 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Privacy_Intl_EFF.pdf (accessed August 20, 2023), pp. 9-10.

create complexity that undermine the objective of mutual legal assistance reform.[70] The presence of multiple competing options for international cooperation also creates avenues and incentives for law enforcement to pick the option of least resistance, frequently to the detriment of human rights.[71]

50. We recommend limiting the scope of Chapters IV-V so that these chapters and their underlying provisions only apply to offences established in accordance with Articles 6 to 16.

Articles 40(4), 42-26, 47 and 54: Overbroad global cooperation powers

Recommendation 11: Amend Article 40(4) to exclude proactive cross-border disclosure of personal data, amend Articles 42-46 so that mutual legal assistance is carried out in accordance with safeguards and limitations set out in Chapter IV of the Draft Text, amend Articles 44 and 45 to allow refusal of requests for mutual legal assistance on the basis of the grounds contained in Article 40(21), remove Articles 47(1)(b) and (c), remove Article 47(1)(g) or, at minimum, amend it to exclude any sharing of personal data, amend Article 47(1)(d) to remove information sharing regarding the use of privacy-enhancing tools, and amend Article 54 to incorporate safeguards against human rights abuses. [51-56]

51. A number of the Draft Text's substantive provisions do not incorporate sufficient human rights protections and are particularly at risk of significant abuse.

52. Articles 40(4)-(5) authorize proactive information disclosures without any consideration for the safeguards of sending or recipient states. This provision raises a particularly heightened threat to online anonymity to the degree it allows proactive disclosure of subscriber data.[72] Despite limits in Article 40(5), the provision also creates problematic opportunities for parallel construction[73] and particularly as there is no requirement that proactively shared information be vetted by a recipient country's central authority in writing prior to being sent to law enforcement agencies nor are the standard grounds for refusal set out in Article 40(21) incorporated. To prevent abuse of this provision, any proactive sharing of personal information should be excluded:

> Amend Article 40(4) by adding "… State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where … could result in a request formulated by the latter State Party pursuant to this Convention **and where the information does not include any personal data**."

53. Articles 42-46 adopt a number of obligations for mutual legal assistance that overlap with powers outlined in Chapter IV but without incorporation of any of the limitations and safeguards included in Chapter IV. In addition, Articles 44 and 45 should be amended to incorporate conditions and limitations on mutual legal assistance included in Articles 35 and 40, including refusal of requests on the basis of grounds contained in Article 40(21). We recommend consolidating these limitations and safeguards in Article 46*bis* and amending Articles 42-46 accordingly:

---

[70] United Nations Security Council Counter-Terrorism Committee Executive Directorate, "The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspective," CTED Trends Report, January 2022, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf (accessed August 20, 2023).

[71] Ibid.

[72] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, May 22, 2015, https://undocs.org/en/A/HRC/29/32 (accessed August 20, 2023), paras. 47 et seq; *Benedik v. Slovenia*, European Court of Human Rights, App No 62357/14, Judgment, April 24, 2018, https://hudoc.echr.coe.int/eng?i=001-182455 (accessed August 20, 2023), paras. 119 and 126-129; *R v. Spencer*, Supreme Court of Canada, [2014] 2 S.C.R. 212, Judgment, June 13, 2014, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do (accessed August 20, 2023).

[73] Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases* (New York: Human Rights Watch, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases (accessed August 20, 2023).

Article 46*bis*. Safeguards and limitations

1. Mutual legal assistance provided further to Articles 42 to 46 shall be governed by the conditions and procedures provided for under domestic law, limitations imposed in Articles 25 to 30, and safeguards and conditions imposed in Article 24, and shall only be provided to the extent permitted under applicable treaties and domestic law.

2. Mutual legal assistance provided further to Articles 42 to 46 shall respect conditions and limitations imposed in Articles 35 and 40 and shall be subject to refusal on the basis of the grounds contained in Article 40(21).

54. Article 47 adopts a number of requirements for direct law enforcement cooperation.[74] Article 47(1)(b) requires direct sharing of information including the identity, whereabouts and activities of persons suspected of offences. Similar cross-border information sharing mechanisms have been abused to locate and identify political dissidents in diaspora communities as a precursor to harassment and other forms of transnational repression.[75] Article 47(1)(f) requires open-ended information sharing "for the purpose of early identification" of offences covered by the Convention even though many early investigative steps can be highly intrusive.[76] These provisions include no limitations, no protections for the right to privacy and the right to data protection, no safeguards for particularly vulnerable persons such as asylum seekers,[77] and no requirement for central authorities to vet information prior to disclosure and refuse on the basis of grounds outlined in Article 40(21) or where doing so would pose a threat to human rights.

55. Article 47(1)(c) requires the sharing of "necessary items or data for analytical or investigative purposes." This type of open-ended and generalized information sharing poses a substantial risk to human rights. Analytical models in particular will frequently involve deeply sensitive information collected without appropriate the types of limitations that are normally in place for investigations of specific offences.[78] Article 47(1)(d) requires information sharing regarding "means of concealing activities" used to commit offences, opening the door to information

---

[74] Privacy International and Electronic Frontier Foundation, "Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V & VII," July 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Privacy_Intl_EFF.pdf (accessed August 20, 2023), pp. 11-12.

[75] For example, Interpol Red Notices are issued "in order to seek the location of a wanted person and his/her detention, arrest or restriction of movement" See INTERPOL, Rules on the Processing of Data, III/IRPD/GA/2011 (2019), https://www.interpol.int/en/content/download/5694/file/24%20E%20RPD%20UPDATE%207%2011%2019_0k.pdf (accessed August 20, 2023), art. 81; see also art. 88 with respect to Blue notices). Interpol notices and diffusions are subject to advance screening including for human rights compliance by Interpol and review by the Commission for the Control of Interpol's Files (CCF), which is also currently reviewing Interpol's policies for personal data sharing in relation to Blue notices. See INTERPOL, "Activity Report for the Commission for the Control of Interpol's Files for 2021," CCF/122/12, https://www.interpol.int/en/content/download/18398/file/CCF%20Annual%20Report%20for%202021-ENG.pdf (accessed August 20, 2023), para. 16 and appendix, paras. 14-18. Each year, hundreds of red notices are found to be faulty and abuse of red notices has led to severe human rights violations, often as part of a broader campaign of surveillance and repression directed at diaspora communities. See Letter from Human Rights Watch to Interpol Secretary General Stock, "Re: Concerns Regarding Interpol and China," September 24, 2017, https://www.hrw.org/news/2017/09/24/letter-hrw-interpol-secretary-general-stock (accessed August 20, 2023); "Hakeem Al-Araibi's case is a true test of Fifa's new huma rights policy," Human Rights Watch news release, December 6, 2018, https://www.hrw.org/news/2018/12/06/hakeem-al-araibis-case-true-test-fifas-new-human-rights-policy; Human Rights Watch, World Report: Tajikistan: Events of 2018, https://www.hrw.org/world-report/2019/country-chapters/tajikistan (accessed August 20, 2023); Yana Gorokhovskaia and Isabel Linzer, "Policy Responses to Transnational Repression," Freedom House, June 2022, https://freedomhouse.org/sites/default/files/2022-05/TransnationalRepressionReport2022_CaseStudy_United_States_NEW.pdf (accessed August 20, 2023), p 9. Article 4(1)(b) provides no screening process, no vetting mechanisms, and does not even obligate agencies to provide sufficient data to assess the information-sharing mechanism is being abused. See also National Immigrant Justice Center, Cristosal, Access Now and International Human Rights & Conflict Resolution Clinic, Stanford Law School, "Request for an Investigation into the Department of Homeland Security's Reliance on Noncredible Information Provided by Human Rights Abusing Authorities in El Salvador," June 6, 2023, https://immigrantjustice.org/sites/default/files/uploaded-files/no-content-type/2023-08/Complaint%20Re%20El%20Salvador%20Data-Sharing%20Agreements%20-%20Web_0.pdf (accessed August 20, 2023).

[76] *United States v. Carpenter*, 585 US __ (Supreme Court of the United States, 2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (accessed August 20, 2023), p. 20, per Kennedy, J, dissenting.

[77] Asylum seekers are particularly at risk of being exposed in this manner: *J.S. v Australia*, November 21, 2022, CCPR/C/135/D/2804/2016, https://undocs.org/en/CCPR/C/135/D/2804/2016 (accessed August 20, 2023), para. 8.2.

[78] ARTICLE 19, "Comments on the "Zero Draft" of the UN Cybercrime Convention," July 2023, https://www.article19.org/wp-content/uploads/2023/07/ARTICLE-19-analysis-of-the-Cybercrime-Convention-Zero-Draft-Final.pdf (accessed August 20, 2023), pp. 9-10.

sharing aimed at undermining general purpose privacy enhancing tools such as VPNs and encryption safeguards. We would therefore recommend that:

> Articles 47(1)(b) and (c) be removed and that Article 47(1)(f) be limited in application to "exchange of information **that is not personal data**" or removed altogether. Article 47(1)(d) should be amended to remove "and other means of concealing activities."

56. Article 54 creates a vehicle for technical assistance and capacity building but does not include any measures to prevent human rights abuses.[79] We support the recommended amendments to Article 54 proposed by EFF and PI.

[79] Privacy International and Electronic Frontier Foundation, "Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V & VII," July 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Privacy_Intl_EFF.pdf (accessed August 20, 2023), pp. 13-14.