Privacy International and Electronic Frontier Foundations' Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty

December 2022

Introduction

Privacy International (PI) is a non-governmental organization in consultative status with ECOSOC. PI researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilizes allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

Electronic Frontier Foundation (EFF) is a nonprofit organization defending human rights in the digital world. Founded in 1990, EFF champions human rights through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports human rights, justice, and innovation for all people of the world.

PI and EFF welcome the opportunity to submit their observations to the "consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement" of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" (hereinafter "consolidated text") before the fourth session of the Ad-Hoc Committee in January 2023. While PI and EFF are not convinced a global cybercrime treaty is necessary, we advocate for having a human-rights-by-design approach in the proposed UN Cybercrime treaty.

In the following sections, we provide our observations and recommendations on some of the provisions included in the consolidated text.

Chapter I – General Provisions

PI and EFF noted in its intervention before the Ad-Hoc Committee that, even as cybercrimes often threaten peoples' rights, risks to human rights have also arisen from vague and overbroad definitions of criminal offenses, and abusive applications of criminal law taken in the name of combating cybercrime. Similarly, the Office of the High Commissioner for Human Rights raised concerns about "the common use at national levels of cybercrime laws and policies to restrict freedom of expression, target dissenting voices, justify Internet shutdowns, interfere with privacy and anonymity of communications, and limit the rights to freedom of association and peaceful assembly."[1] The discussions at the prior sessions of the Ad-Hoc Committee have shown that there is yet no shared global consensus on how to define cybercrime.

Similarly, the scope of application of the procedural measures and law enforcement (including collection and transfer of evidence) should be limited to addressing cybercrime, not the full range of criminal conduct, in order to avoid investigative powers and procedures being used for less serious crimes or crimes that may not be consistent with States' human rights obligations. The proposed Convention is about addressing cybercrime, not a general-purpose law enforcement treaty.

Further, PI and EFF are concerned with the wording of Article 3.3 of the consolidated text. As drafted, the provision states that "it shall not be necessary [...] for the offenses [...] to result in damage or harm to persons, including legal persons, property and the State." This wording increases the likelihood of prosecuting individuals for behaviour that did not, or could not have been expected to, cause harm or damage.

As for the protection of sovereignty in Article 4, PI and EFF reiterate that, when conducting an extraterritorial surveillance measure (such as hacking), government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use extraterritorial measures (such as hacking) to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These

[1] See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

mechanisms must be clearly documented, publicly available, and subject to guarantees of procedural and substantive fairness.[2]

For these reasons, we recommend that:

- The purpose of the future treaty is to promote and to strengthen measures to prevent and combat cybercrime (Article 1);

- Cybercrime is defined as offenses in which information and communications technologies (ICTs) are the direct objects as well as instruments of the crimes (cyber-dependant crimes, i.e. crimes that could not exist at all without the ICT systems.) (Article 2);

- The scope of application of this Convention is the prevention, detection, investigation, and prosecution of cybercrime as defined; and applies to the collecting, obtaining, preserving, and sharing of evidence in electronic form of cybercrime as defined in the Convention (Article 3);

- Article 3.3 should be deleted completely or reworded. The default assumption should be to require malicious or fraudulent intent and harm for a violation to occur. Otherwise, trivial violations or even beneficial security or journalistic research can be made criminal. While certain crimes do not need to prove economic or physical harm, for example, interception of private communication, those should be expressed within the definition of that specific crime.

We welcome the provision in Article 5 on respect for human rights and the inclusion of gender perspectives. However, we note the need to include that specific safeguards to ensure the respect of human rights is included in other provisions of the proposed Convention. We make specific recommendations in the following sections in Chapters III and IV of the consolidated text. Failing to reflect these safeguards risks creating a disconnect between the general obligation under Article 5 and those contained in other articles of the Convention — a disconnect that risks creating legal uncertainty and that can be exploited by those governments seeking to justify laws and practices that do not comply with human rights.

[2] See https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf

Chapter II – Criminalization

As noted in the observations under Chapter I above, the scope of criminal conduct covered under the definition of “cybercrime” should be narrow, precise, and specific. It follows that this chapter should only cover core cybercrimes, i.e. offenses in which ICTs are the direct objects as well as instruments of the crimes; these crimes could not exist at all without the ICT systems. A useful reference for the types of crimes that are inherently ICT crimes can be found in Articles 2-6 of the Budapest Convention: illegal access to computing systems, illegal interception of communications, data interference, system interference, and misuse of devices. For example, spreading a computer virus in the wild, breaking into the computer system of a bank to steal money, and using malicious software to delete all the data of a former employer’s systems.

Further, criminal conduct, such as illegal access, should require malicious/fraudulent intent and harm. Standards such as “without authorization” or "unlawfully" risk allowing the criminalisation of acts carried out with beneficial intent, such as security research, and increase the likelihood of prosecuting individuals for behaviour that did not, or could not have been expected to, cause harm or damage.

For these reasons, we recommend to:

- Include in the Convention only crimes listed in Cluster 1 of the consolidated text (Articles 6 to 10);

- Include the standard of malicious/fraudulent intent and harm in Article 6 and Article 10 of the Convention.

- Article 6(3)(b) should only cover specific types of confidential information, like highly classified information.

Should other non-cyber dependent crimes be included, we recommend that cyber-enabled crimes are narrowly defined and consistent with international human rights standards. The Convention should not seek to cover ordinary crimes already clearly and adequately prohibited under existing domestic legislation and merely incidentally involve or benefit from ICT systems without targeting or harming those systems. For example, “drug trafficking,” “arms trafficking,” “distribution of counterfeit medicines,” and “money laundering” are already crimes, and a computer may merely have been used to communicate about an offense (see some of the crimes listed in Clusters 2 and 10).

We are particularly concerned about the potential inclusion of content-related offenses (see examples under Clusters 4, 7, 8, and 9). Including these crimes poses a heightened risk that the proposed Convention will be used to prohibit expression that is protected under international human rights standards. Further, we are concerned at the inclusion of "extremism-related offenses" (Article 27) and "terrorism-related offenses" (Article 29). There are no internationally agreed definitions for these crimes, and many states justify human rights repressive practices, such as the prosecution of political opponents, human rights defenders, and journalists, the unlawful restriction of the exercise of the rights to freedom of expression and peaceful assembly, and the unlawful interference with the right to privacy, on the basis of broad, ill-defined crimes under their national legislation.

Chapter III - Procedural measures and law enforcement

Article 41 - Scope of procedural measures

Widening the scope of all crimes committed with the use of an ICT significantly risks undermining human rights, including the right to privacy and the right to a fair trial. As the 2022 UN Security Council's Counter-Terrorism Committee Executive Directorate noted, in attempting "to address law enforcement's jurisdictional problems, the substantive law will become weakened, giving law enforcement too-quick access with too-little due process."[3]

For the reasons illustrated in the comments to Chapter I above, we recommend that the scope of procedural measures is limited to the investigation of the criminal offenses established in accordance with this Convention.

Article 42. Conditions and safeguards

We welcome the reference in this provision to "adequate protection of human rights and liberties" and the requirement to incorporate in national laws "the principles of proportionality, necessity and legality and the protection of privacy and personal data," However, we note that this article is fundamental as it aims to provide the safeguards which are applicable to the investigative powers contained in Articles 43 to 49. Hence it is necessary that additional safeguards are included and existing ones are further clarified and strengthened to avoid the risk of human rights abuses in the applications of these powers.

[3] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), The state of international cooperation for lawful access to digital evidence: Research Perspectives, January 2022, available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_tre nds_report_lawful_access_to_digital_data_.pdf

Specifically, we recommend that Paragraph 2 of Article 42 is strengthened to require not only independent supervision but also prior independent (preferably judicial) authorisation of surveillance measures that interfere with the right to privacy. This would bring the paragraph in line with existing jurisprudence of human rights courts and bodies.[4]

Further, this Article should make clear that the test of legality, necessity, and proportionality and the requirements of prior independent (preferably judicial) authorisation and post ante independent monitoring apply to all types of personal data, including non-content data such as metadata, traffic data, and subscriber information. Non-content data, when collected in aggregate about one or several individuals, is no less—and can be even more—sensitive than the actual content of communications.[5] This data makes it possible to know the identity of the person with whom a subscriber or registered user has communicated and by what means, as well as identify the time of the communication and the place from which that communication originated. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.[6] Subscriber information can be used to identify individuals associated with online activity. As a result, communications data, including metadata, should enjoy at least the same protections as content, and access to this data should be subject to the same conditions and protections as any other personal information.

In addition, we recommend that this Article is significantly expanded to cover the following safeguards:

- Right to an effective remedy. As noted in the report of the UN High Commissioner for Human Rights, The right to privacy in the digital age, effective remedies for violations of privacy "must be known and accessible to anyone with an arguable claim that their rights have been violated." In particular, the High Commissioner stated that "notice (that either a general surveillance regime or specific surveillance measures are in place) and

[4] See Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

[5] See UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020) "Noting that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity," See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021), "Acknowledging that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, including their movements, social relationships, political activities, private preferences and identity,"

[6] See Privacy International, ARTICLE 19, and the Electronic Frontier Foundation Intervention in Pietrzak v Poland, https://privacyinternational.org/legal-action/pietrzak-and-others-v-poland

standing (to challenge such measures) thus become critical issues in determining access to effective remedy." Further, the effective remedies must include "prompt, thorough and impartial investigation of alleged violations" and such independent investigative bodies need to have the power to order the end of ongoing violations as well as "full and unhindered access to all relevant information, the necessary resources, and expertise to conduct investigations and the capacity to issue binding orders."[7]

- A provision to require that any investigative powers listed in this Convention must be conducted in ways that do not compromise the security of digital communications and services. We are particularly concerned with ensuring that this Convention does not in any way justify government hacking. Government hacking should be outside the scope of this treaty because it is unlike any other form of existing surveillance technique. Government hacking can be far more privacy intrusive than any other surveillance technique, permitting remote and secret access to personal devices and the data stored on them, as well as the ability to conduct novel forms of real-time surveillance, for example, by turning on microphones, cameras, or GPS-based locator technology. Hacking also allows governments to manipulate data on devices, including corrupting, planting, or deleting data, or recovering data that has been deleted, all while erasing any trace of the intrusion. It not only poses unique privacy interference to the intended targets, but it often affects the privacy and security of others in unpredictable ways. Hacking is about causing technologies to act in a manner the manufacturer, owner, or user did not intend or did not foresee. In its most dangerous form, government hacking depends on exploiting unpatched vulnerabilities in systems to facilitate surveillance objectives. This is, therefore, fundamentally at cross-purposes with digital security aims: in the surveillance context, the government identifies vulnerabilities, not to secure systems through testing and coordinated disclosure but to exploit them in order to facilitate a surveillance objective. This approach not only undermines the security of the target system but also of other systems.[8]

[7] See UN Doc A/HRC/27/37.

[8] See report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, UN doc. A/HRC/51/17, August 2022. For PI's safeguards on government hacking: https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf

Article 43. Expedited preservation of [stored computer data][accumulated digital information]

We recommend that this article include the requirement that expedited preservation is only conducted when "there is a reasonable belief that a criminal offense was committed or is being committed."

Article 46. Search and seizure of [information stored or processed electronically] [stored computer data]

The current wording of Article 46(4) raises concerns with regard to potential obligations imposed upon third-parties, such as communication services providers, to either disclose vulnerabilities of certain software or to provide relevant authorities with access to encrypted communications. It should be noted that, if authorities are allowed to exploit such gaps, they will more likely than not have an interest in building an "arsenal" of security gaps in order to be able to attack a target in the event of an investigation. This interest, in turn, will prevent them from notifying the affected manufacturer of IT systems, who can help close the security gap that has been discovered. If this happens, it means that the worldwide security risk would far outweigh the possible facilitation of prosecution in individual cases.

Moreover, requirements imposed on service providers that would essentially compromise existing security standards in communications might equally constitute a serious interference with, among others, the right to privacy. International human rights law requires states to abstain from such interferences or even take measures to ensure a high level of security, integrity, and confidentiality of communications within the context of their positive obligations.

Article 47. Real-time collection of traffic data

Blanket or indiscriminate measures that provide for generalised interception, storage, or retention of the content of communications or accompanying metadata have been deemed to fail to satisfy the principle of necessity and proportionality, and have several times been deemed to be against human rights laws by both national and international courts, including the Court of Justice of the EU and the European Court of Human Rights, as well as independent UN human rights experts.[9]

[9] For references to relevant jurisprudence see Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

We thus recommend this Article clarifies that the powers in Article 47 paragraph 2 refer only to "such data associated with specified information in the territory of that State Party" (as per paragraph 1) to avoid any risks that this provision may be interpreted to justify the imposition of indiscriminate data retention obligations on service providers.

Article 48. Interception of content data

For the reasons illustrated in the comments on Chapter I, we recommend that paragraph 1 of this Article is worded in such a way as to be limited to the investigation of the crimes defined in this convention.

Further, we recommend that this Article clarifies that the interception of content data is only conducted when "there is reasonable belief that a criminal offense was committed or is being committed."

As for the provision in paragraph 3, we have the same concern as those expressed for Article 47 above.

Article 49. Admission of [digital] [electronic] evidence

This Article, as currently worded, is very broad and provides no meaningful safeguards to ensure that the evidence collected and admitted complies with international human rights law, including the right to a fair trial and the right to privacy. This is a significant gap given the practices of some states to extract evidence from people's personal devices in ways that are unregulated. For example, PI documented how mobile phone extraction tools enable police and other authorities to download content and associated data from people's phones.[10] This can apply to suspects, witnesses, and even victims of crime – often without their knowledge or consent.[11] Increasingly mobile phone extraction can be used to target protestors without an appropriate legal framework or safeguards.[12]

[10] See https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

[11] The risks that this surveillance technology poses are well illustrated in the case brought by asylum seeking claimants in the UK, which resulted in a High Court ruling in 2022 that the UK government acted unlawfully and breached human rights and data protection laws by operating a secret, blanket policy of seizing, retaining and extracting data from the mobile phones of asylum seekers arriving by small boats, see https://privacyinternational.org/news-analysis/4987/uk-high-court-orders-groundbreaking-redress-thousands-migrants-affected-unlawful

[12] Other countries are reportedly using such capabilities, e.g. Argentina, https://adc.org.ar/informes/quien-revisa-tu-telefono/