Electronic Frontier Foundations and Privacy International

Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty: Chapters on International Cooperation, Technical Assistance, and Proactive Measures

March 2023

Introduction

Electronic Frontier Foundation (EFF)[1] and Privacy International (PI)[2] welcome the opportunity to provide observations and recommendations on the proposed consolidated negotiating document for the fifth session of the Ad Hoc Committee. Our submission covers provisions in the chapters related to the preamble and international cooperation of the proposed "comprehensive international convention on countering the use of information and communications technologies for criminal purposes." We also provide comments on Article 42 from the criminal procedural measures and law enforcement chapter discussed in the fourth session, as it is of significance to the international cooperation chapter. In the following sections, we provide our recommendations and rationale for provisions in the consolidated text.

I. General Recommendation: The Proposed UN Cybercrime Convention Should be Built On a Foundation of Human Rights

[1] Electronic Frontier Foundation (EFF) is a nonprofit organization defending human rights in the digital world, and registered under operative #9. 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 everyone.

[2] 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.

EFF and PI strongly recommend that human rights safeguards should form a baseline for both the criminal procedural measures and international cooperation chapters. The use of existing and new technologies and the vast amount of personal data available present both opportunities and challenges for law enforcement authorities in gathering potential evidence during criminal investigations, including across borders. While digital evidence can be crucial for solving and prosecuting cybercrimes, its collection and use can also implicate human rights, including the right to privacy and personal data protection. Therefore, it is necessary to establish clear human rights safeguards to ensure that procedural measures and international cooperation between law enforcement agencies respect international human rights standards and are lawful, necessary, and proportionate.

Regrettably, many States already fall short in this regard, failing to uphold human rights, including the right to privacy and data protection. In some cases, surveillance laws have been used to justify overly broad surveillance practices that disproportionately target individuals or groups based on their political views, particularly ethnic and religious groups, leading to the suppression of free expression and association and the silencing of dissenting voices. We have seen how the COVID-19 pandemic has provided authorities with an opportunity to institute intrusive forms of surveillance without appropriate checks and balances. Examples of abusive practices include covert surveillance of internet activity without a warrant, using surveillance technology to track individuals in public, and monitoring private communications, all without legal authorization, oversight, or any other safeguard. Personal data on religious beliefs, political affiliations, and other sensitive information is collected without guardrails against abuses.

Checks and balances are essential to avoid abuse of power. First, the principle of legality is a fundamental aspect of international human rights instruments and the rule of law in general. It is an essential guarantee against the state's arbitrary exercise of its powers. Second, the principle that any interference with a qualified right, such as the right to privacy or freedom of expression, must be necessary and proportionate is one of the cornerstones of human rights law.[3] In general, it means that a state must not only demonstrate that its interference with a person's right meets a "pressing social need" but also that it is proportionate, or under Inter-American jurisprudence adequate, to the legitimate aim pursued. Third, decisions relating to communications surveillance should be made by a competent judicial authority acting independently of the government. This reflects the core requirement of international human

[3] For a compendium of relevant international and regional human rights standards, resolutions and jurisprudence, see Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

rights law that the use of lawful surveillance powers by public officials must be not only necessary and proportionate but also be attended by independently monitored, strict safeguards against abuse. Prior judicial authorization of surveillance powers is not merely desirable but essential. This is because neither of the other two branches of government can provide the necessary degree of independence and objectivity to prevent the abuse of surveillance powers. Fourth, "user notification and transparency" safeguard the right to privacy by compelling governments to notify people who have been surveilled, allowing people to challenge government interference with their privacy and protecting their rights to an effective remedy and fair trial. Fifth, public oversight, another key check, relates to the importance of transparency in a democracy. It is essential that persons have sufficient information on how laws are working, including through audits, spot checks, and transparency oversight reports. Sixth, the right to privacy entails the right of persons to construct means of communicating with one another secure from outside intrusion. The duty of governments to respect the privacy of communications also imposes a corresponding obligation on those governments to respect the integrity of any and all systems used to transmit private communications.[4]

Respecting human rights is not only a legal obligation but also a practical necessity for law enforcement. As the Office of the High Commissioner for Human Rights (OHCHR) said in its "Human Rights and Law Enforcement: A Trainer's Guide on Human Rights for the Police," law enforcement agencies' effectiveness is improved when they respect human rights. When police officers consistently respect human rights, they become more "professional[] in their approaches to solving and preventing crime and maintaining public order." Thus, "respect[ing] for human rights [...] is a moral, legal, and ethical imperative [but also] a practical necessity for law enforcement." When law enforcement authorities "respect, uphold, and defend human rights," the OHCHR guide explains, several positive outcomes occur, including enhancing "public confidence [...] and community cooperation," achieving successful prosecutions in court, being "seen as part of the community, performing a valuable social function," promoting "fair administration of justice," and setting "[a]n example [...] [for] respect for the law."[5] Moreover, as the Vienna Declaration and Programme of Action note, "The administration of justice, including law enforcement [...] agencies, [...] in full conformity with applicable standards contained in international human rights instruments, [is] essential to the full and

[4] Abstract from Electronic Frontier Foundation and ARTICLE19, Necessary & Proportionate Global Legal Analysis, (May 2014). https://necessaryandproportionate.org/global-legal-analysis/
[5] United Nations, Human Rights, and Law Enforcement A Trainer's Guide on Human Rights for the Police, New York, 2002, https://www.ohchr.org/sites/default/files/Documents/Publications/training5Add2en.pdf

non-discriminatory realization of human rights and indispensable to the process of democracy and sustainable development."[6]

In conclusion, we strongly recommend that human rights safeguards under Article 42 be the baseline for the scope of the international cooperation chapter.

II. Recommendation to Strengthen Human Rights Conditions and Safeguards

We recommend the additions in brackets to strengthen the protections for human rights and fundamental freedoms, including privacy and personal data, in implementing the powers and procedures outlined in Article 42, as follows:

Article 42: Conditions and Safeguards

> .~~Such c~~Conditions and safeguards for ~~shall, as appropriate in view of the nature of~~ [the] procedure[s] or power[s provided for in this Convention shall] ~~concerned, inter alia,~~ include judicial or [similar] independent [civilian] ~~supervision~~ [authorization. Regardless of the nature of the procedure or power concerned, limitations on the scope and duration of such power or procedure, effective redress mechanisms, and independent oversight bodies with authority to conduct audits, spot checks, impose redress measures, and annual public reporting shall be in place. Measures preventing a service provider from disclosing the execution of any power or the existence of an investigation should be an exceptional measure, limited in duration, and subject to strict criteria with clear and compelling reasons for imposing such restrictions. Any grounds justifying the application of such powers shall be based on a strong evidentiary showing. Powers and procedures provided for in this Convention shall not undermine the security and integrity of digital communications and services.]
>
> 3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this article upon the rights, responsibilities, and legitimate interests of third parties.

[6] Vienna Declaration and Programme of Action, World Conference on Human Rights in Vienna, 1993, https://www.ohchr.org/en/instruments-mechanisms/instruments/vienna-declaration-and-programme-action

Rationale: Separating the conditions and safeguards, as suggested in the proposed amendments, into two sentences allows for a more organized presentation and emphasizes the importance of effective redress mechanisms and independent oversight as cross-cutting obligations under existing international human rights law, as reaffirmed in resolutions of the UN General Assembly and Human Rights Council.[7] Regarding the grounds justifying application, we recommend changing the qualifier "as appropriate in view of the nature of the procedure or power concerned" to clarify that the conditions and safeguards expressed in this article apply to all procedures or powers provided in the Convention.

III. Recommendations for the Preamble

We recommend adding the following new recitals to the Preamble section:

- [Noting with great concern that the use of existing and new technologies processing vast quantities of personal data has created new challenges for the protection of human rights and fundamental freedoms in the context of criminal investigations, particularly the right to privacy and the protection of personal data,]

- [Recognizing that human rights and fundamental freedoms are implicated by how, and under what circumstances, law enforcement authorities are allowed to secure potential evidence during a criminal investigation, including across borders,]

Rationale: States should recognize the rapid and dramatic technological changes that have often reshaped the nature and scope of criminal investigations, including the associated challenges for the protection of human rights.[8] While it is important to ensure that law enforcement authorities have the necessary tools to gather potential evidence in cybercrime cases, these tools should always be used in a manner that is consistent with international human rights law.

We recommend modifying the Preamble's fifteenth existing recital as follows:

---

[7] UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/74/147 (18 December 2019); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019).

[8] For an overview of some of the challenges related to the use of existing and emerging technologies, see reports of UN High Commissioner for Human Rights on the right to privacy in the digital age, and report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism referenced in the Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

["~~Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for human rights as enshrined in applicable~~ Recognizing that law enforcements powers and procedures are subject] to international and regional human rights conventions and treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning respect for privacy."

We recommend modifying the Preamble's sixteenth existing recital as follows:

["~~Mindful~~ Acknowledging also ~~of~~] the right to the protection of personal data, which helps individuals exercise control over information relating to themselves that may be unlawfully collected and used by others.

Rationale: While it is true that other international treaties, such as the Budapest Convention, may use the term "mindful" to refer to a similar provision to the sixteenth one of the present Preamble, we believe that this proposed Convention should specifically and firmly acknowledge the importance of human rights in the context of criminal investigations related to cybercrime. By doing so, this treaty can set a clear and firm commitment for member states to their international human rights obligations.

IV. Recommendations for Cluster I - International Cooperation Chapter

Article 56. General principles of international cooperation

We recommend amending paragraph 1 of Article 56 by removing the term "reciprocity" and replacing it with "dual criminality." We also recommend that the international cooperation components of the Convention be limited in scope to the investigation and prosecution of specific crimes itemized in the Convention. In the scenario that Member States decide to extend the scope of cooperation beyond those specific crimes, the proposed Convention should be limited, at minimum, to "serious crimes" in similar terms to Article 2 of the United Nations Convention against Transnational Organized Crime. Specifically, the definition should refer to an offense punishable by a maximum deprivation of liberty of at least four years or a more severe penalty.

1. State Parties shall cooperate to the fullest extent possible in accordance with the provisions of this chapter, other international instruments on international cooperation in criminal

matters, and agreements based on the principle of [~~reciprocity~~ dual criminality], as well as domestic laws, with a view to [preventing,] detecting, [~~disrupting~~,] investigating, prosecuting and adjudicating offences established in accordance with this Convention and to collecting, obtaining, preserving and sharing evidence in electronic form of [offences set forth in this Convention] [~~any criminal offence~~] [serious crimes].

Rationale: Adding dual criminality would ensure that international cooperation is based on the principle that assistance can only be granted if the conduct in question is a criminal offense under the laws of both the requesting and the requested state parties.

2. States Parties shall consider assisting each other in investigations of and proceedings in civil and administrative matters [strictly and directly] relating to the offenses established in accordance with this Convention, as appropriate and as permitted by their domestic legal systems.

Rationale: The powers and procedures outlined in the present Convention are highly intrusive. By removing paragraph 2 of Article 56, we can ensure that the scope of the Convention remains limited to criminal matters.

3. In matters of international cooperation, ~~whenever~~ dual criminality shall be ~~is~~ considered a requirement, and ~~it shall be~~ deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as that of the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties.

Rationale: Our amendment to paragraph 3 clarifies that dual criminality ensures that international cooperation is based on the principle that assistance can only be granted if the conduct in question is a criminal offense under the laws of both State Parties, irrespective of whether the category or name of the conduct is identical.

4. The powers and procedures provided for in this chapter shall be subject to the conditions and safeguards provided for in Article 42.

Rationale: We support keeping paragraph 3 of Article 42 intact. However, we recommend that Article 42 be strengthened as outlined in the first recommendation of the present submission to

ensure that the powers and procedures provided for in the chapter are subject to appropriate conditions and safeguards to protect against potential human rights abuses.

Article 57. [~~Protection of personal data~~ Data Protection and Transfer of Personal Data]

1. Personal data may only be transmitted from one State Party to another State Party on the basis of a request made in accordance with this Convention for the purpose of a specific criminal investigations or proceedings and may only be used by the State Party to which the data are transmitted for the purposes of criminal, administrative, or civil proceedings and other judicial or administrative procedures [strictly and] directly related to ~~those~~ [the initial criminal] proceedings that justified transmission, as well as to prevent an imminent and serious threat to the [life or safety of any individual] ~~public safety~~ of those persons whose personal data are transmitted.

7. This Article does not provide a complete accounting of all measures that may be required to ensure adequate protection of personal data and is without prejudice to conditions on the transferring of personal data to other States imposed in any Parties' domestic legal framework or to the adoption of additional safeguards to meet State Parties' obligations under Article 42 of this Convention.

Rationale: Amending the article's title could help to more accurately reflect the article's content, which deals with transferring personal data between States Parties. Regarding the proposed amendment to paragraph 1 of Article 57, we recommend adding the word "strictly" before "directly" to emphasize that the use of personal data should be limited to only those proceedings that are strictly related to the original request and to clarify that personal data can be used to prevent an imminent and serious threat to life and safety of a person. We recommend deleting the term "public safety," which is often vague and may lead to broad interpretations of the scope and limits of the present article.

Finally, we recommend adding paragraph 7. Many States have data protection laws that impose limits on the transfer of personal data to other States ("third country transfers"). Conditions in such legal frameworks will have to be satisfied through bilateral or multilateral agreements between Parties.

V. Recommendations for Cluster 6

~~**Article 64. Spontaneous information**~~

Rationale: We recommend deleting Article 64. The proposed provision disregards several safeguards already present in the Convention that are crucial to upholding human rights. By making the transmitting state's domestic law the primary determinant of whether information can be disclosed, it bypasses significant limitations under this Convention. Moreover, many of the Convention's safeguards are reliant on a formal request for information, as outlined in Article 57(1), 61(6)-(28), and particularly 61(10), which requires central authority participation in cross-border information exchanges. By providing a legal basis for informal information exchanges without an explicit request, this provision also undermines the safeguards of Mutual Legal Assistance regimes, which are triggered by explicit requests for information. As a result, there is no mechanism for the receiving state to assess the human rights implications of the investigative methods used by the sending state to obtain the information, with severe consequences for human rights.

Sub-clause 2 raises additional concerns by allowing State Parties to share information and demand its confidentiality. Although sub-clause 2 permits State Parties to refuse confidentiality if it conflicts with the receiving State's obligation to disclose exculpatory evidence in criminal proceedings, this caveat falls short in several respects. First, discovery obligations in criminal proceedings require the disclosure of all evidence that the State used in developing its case, even if the evidence is not exculpatory. This is significant because incriminating evidence obtained in violation of constitutional principles can often taint other evidence-gathering processes or justify abuse of process claims. Withholding incriminating evidence can thus undermine fundamental justice in criminal proceedings. Second, while we acknowledge that confidentiality requests are made before evidence is transmitted, the receiving state will need to understand the content and nature of the evidence to assess whether it can respect the confidentiality request. Even if the evidence is not then transmitted, the receiving state can recreate the evidentiary path because it is aware the evidence exists. This form of parallel construction can seriously compromise the criminal justice system's integrity. We would, therefore, urge the total deletion of this Article.

Article 68. Mutual legal assistance in the expedited preservation of stored [computer data] [electronic/digital information]

2. A request for preservation made under paragraph 1 shall specify:

(b) The offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts [providing reasonable grounds to believe that a criminal offense has been or will be committed and that the data sought is likely to yield evidence of that offense];

Rationale: Clarify the circumstances under which a request to preserve electronic data can be made. It provides an additional layer of protection against frivolous or unjustified requests to preserve electronic data.

(g) [If there are independent grounds to believe there is] a need to keep the request for preservation confidential and not notify the user [because disclosure of the request would lead to death, serious bodily injury, or destruction of evidence].

Rationale: Adding paragraph (g) to Article 68 would allow for exceptional circumstances where requests for preservation of electronic data can be kept confidential and not disclosed to the user.

Article 71. Emergency mutual legal assistance in the expedited production of stored [computer data] [electronic/digital information]

The first paragraph 1 of Article 66 (on the definition of an emergency) should also be added as a new first paragraph of Article 71.

1. For the purposes of this article, an emergency means a situation involving a substantial and imminent risk to the life or safety of any individual.

Rationale: Our proposed amendment seeks to define the conditions that can justify an emergency request by drawing an analogy to Article 66(1), which already defines such conditions.

Article 72. Cross-border access with consent or where publicly available

Cross-border access to stored [computer data] [electronic/digital information] with consent or where publicly available [Subject to a reservation,] a State Party may, without the authorization of another State Party:

(a) Access publicly available (open source) stored [computer data] [electronic/digital information], regardless of where the [data are] [information is] located geographically; or

(b) Access or receive, through [a computer system] [an information and communications technology system/device] in its territory, stored [computer data] [electronic/digital information] located in another State Party, if the State Party accessing or receiving the [data] [information] obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the [data] [information] to that State Party through that computer system. [Consent shall not be considered valid if provided by a service provider on behalf of an individual user of the service.]

Rationale: This amendment to Article 72(b) aims to clarify that consent to access or receive stored computer data located in another State Party cannot be obtained by a service provider on behalf of an individual user of the service.

Article 75. Law enforcement cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems [and the conditions and safeguards set out in Articles 42 and 57, to ensure that cooperation is conducted in accordance with international human rights law], to enhance the effectiveness of law enforcement action to combat the offences covered by this Convention. Each State Party shall, in particular, adopt effective measures:

Rationale: Our proposed amendment aims to clarify that cooperation between States should also adhere to international human rights law and standards, which is crucial to prevent any abuse or misuse of power in the process of law enforcement cooperation. As noted by UN General Assembly resolution on the right to privacy in the digital age[9], as well as independent human rights experts, intelligence sharing across borders is often conducted without adequate legal basis and safeguards against abuses.[10]

[9] UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020), which emphasizes "that States must respect international human rights obligations regarding the right to privacy when they intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information- and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including business enterprises".
[10] See Privacy International, Minimum safeguards on intelligence sharing required under international human rights law,

Article 76: Public-private partnerships to enhance the investigation of [cybercrime] [the use of information and communications technologies for criminal purposes]

1. States Parties shall collaborate to conclude bilateral and multilateral agreements or arrangements to assist their respective law enforcement agencies in cooperating directly with relevant service providers in their respective territories through public-private partnerships, with a view to streamlining cooperation with industry and enhancing collaboration between States Parties, Governments, and private service providers to establish modalities or protocols of cooperation in law enforcement, the investigation of [cybercrime] [the use of information and communications technologies for criminal purposes] and evidence collection, in particular for addressing the challenges posed by the cross-border acquisition of electronic evidence.

2. States Parties [~~shall develop guidelines for~~ may encourage] service providers in assisting law enforcement agencies in the investigation of [cybercrime] [the use of information and communications technologies for criminal purposes], including with regard to the format and duration of preservation of digital evidence and information, [while ensuring that such guidelines are consistent with the conditions and safeguards established in Article 42, in addition to other safeguards such as transparency, adequate procurement, accountability, oversight, and redress.]

Rationale: Our amendment aims to remove the obligation on States Parties to develop guidelines for service providers. However, if States prefer to retain Article 76, we suggest amending paragraph 2 to remove the obligation on State Parties to develop law enforcement guidelines. Instead, the paragraph should encourage service providers to publish their own law enforcement guidelines. Nonetheless, any guidelines developed by the service providers should always be consistent, at minimum, with the conditions and safeguards established in Article 42 of the present Convention and domestic legal protections. Privatization of public responsibilities that involve the collection and processing of personal data can pose significant risks to the protection of human rights. Private companies may not be subject to the same level of accountability and oversight as public authorities, which can lead to abuses of individuals' rights. When public-private partnerships (PPPs) involve surveillance technology and mass data processing, detailed safeguards are required to ensure that they are conducted in a manner consistent with international human rights law and standards. These safeguards should go

---

https://privacyinternational.org/advocacy/3068/minimum-safeguards-intelligence-sharing-required-under-international-human-rights-law.

beyond those outlined in Article 42 or our own proposed amendment above. Privacy International has developed detailed safeguards that are targeted to PPPs. Such safeguards are classified between principles of Transparency, Adequate Procurement, Accountability, Legality, Necessity & Proportionality, Oversight, and Redress. Together they seek to uphold human rights and restore trust in the state's public functions, as these increasingly get outsourced to private hands.[11]

Article 77. Joint investigations

> States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to matters that are the subject of investigations, prosecutions, or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. ~~The States Parties involved shall ensure that the sovereignty of the State Party in the territory of which such investigation is to take place is fully respected.~~ Joint investigation teams shall carry out their operations in accordance with the domestic law of the Party in which they operate, as well as Article 42 of the present Convention. Measures shall be in place to ensure joint investigative teams and the agreements that establish respect the conditions and safeguards and principles of mutual legal assistance established in this Convention. Article 77 should explicitly require the approval of a State Party's authority or authorities responsible for mutual legal assistance in approving any agreement referred to in Article 77.

Rationale: Joint investigations should respect the rule of law, and there should be clear safeguards against "forum shopping" or other practices that can undermine human rights protections or criminal procedural safeguards in the State where the investigation is carried out or where individuals targeted by the investigation are residing. Investigative measures should always comply with the domestic legal framework of the State where the investigation is carried out or where individuals are targeted.

~~**Article 78. Special investigative techniques**~~

[11] Privacy International, *Safeguards for Public-Private Surveillance Partnerships*, December 2021, https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf

Recommend: Delete Article 78 entirely. Article 78 is problematic for several reasons. First, it is not clear why this article is included in the Chapter on international cooperation. Sub-clause 1 appears to introduce new obligations for State Parties to adopt investigative techniques in national law. Sub-clauses 2-3 largely replicate cooperative capabilities already present in other parts of the international cooperation chapter. Although sub-clause 4 provides for a previously unspecified authority to 'decide at the international level' whether to use a special investigative technique, nothing in its cooperation mechanisms is specific to the types of special investigative techniques envisioned in sub-clause 1. Moreover, the specific techniques mentioned in sub-clause 4 are not "special" but rather already listed in other parts of the Convention.

Secondly, it contains the undefined term "special investigative techniques" and an open-ended reference to methods "such as electronic or other forms of surveillance." This allows for the use of any surveillance techniques, including those that have not yet been developed or that are inherently disproportionate in nature, and therefore prohibited under international human rights law. Similarly, by requiring Parties to "take such measures as may be necessary to allow for the [...] use" of techniques, it implies an open-ended authorization to exercise powers and even to compel others to assist in that exercise. This is problematic both in terms of foreseeability (a key aspect of the legality principle) and in terms of public scrutiny and accountability.

For example, the current wording of this provision could be used to justify government hacking. As we noted in our submission to the fourth session, 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. 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 system vulnerabilities to facilitate surveillance objectives.[12]

Also, and in stark contrast to the rest of the Convention, which defines required investigative techniques and accompanying limitations in detail, Article 78 largely defers to national law in determining what safeguards should accompany the undefined techniques it requires States to adopt, relying heavily on rules of evidence-gathering as articulated by national courts. This approach is particularly problematic because the Article requires States to adopt cutting-edge and emerging techniques–precisely the types of techniques that require additional caution because national court systems have not yet had the opportunity to rule on the novel techniques in question and because the techniques (which are often both novel and not yet publicly discussed) have not yet been subjected to public scrutiny.

Finally, even where Article 78 explicitly specifies investigative techniques that should be adopted, these are also problematic. Sub-clause 1, for example, specifically mentioned controlled delivery and undercover operations. Controlled delivery and undercover operations raise a heightened risk of entrapment and should not be required techniques without additional safeguards in place. In other areas, Article 78 refers to specific techniques that are already defined in other parts of the Convention but without reference to the safeguards and limitations attached to those provisions. In many states, these types of investigative techniques have been used to conduct flagrant human rights abuses targeting vulnerable communities (e.g. LGBT people). For example, sub-clause 4 mentions the collection or interception and real-time transmission of traffic or content data. Still, all of these are explicitly addressed in detail under other provisions of the Convention (see Articles 47, 48, and 48, which have been sent to informals). It's not clear why these investigative powers or their cross-border implications are mentioned in the context of Article 78 or how the joint decision-making referenced in sub-clause 4 with respect to the use of these investigative techniques would interact with the Convention's other provisions on Joint Investigative Teams and requests for mutual assistance.

[12] For more details, see PI and EFF"s submission to the fourth session, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/PI-EFF_comments_on_consolidated_text_December_2022.pdf