Privacy International and Electronic Frontier Foundation's Comments on the Draft Text of the UN Cybercrime Convention: Chapters IV, V and VII

July 2023

Introduction

Privacy International (PI)[1] and Electronic Frontier Foundation (EFF)[2] welcome the opportunity to provide observations and recommendations on the proposed draft text of the Convention.[3] Our submission covers provisions in the chapters related to procedural measures and law enforcement, as well as international cooperation of the proposed convention. We also provide general comments on Article 54, contained in the chapter dealing with technical assistance and information exchange.

In the following sections, we provide our proposed amendments and rationale for selected provisions in the draft text.

[1] 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.

[2] 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.

[3] See Draft Text of the Convention here:
https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main

Recommendations Related to Chapter IV

1. **Recommendation to ensure that the scope of procedural measures apply only to offences covered by the Convention**

Article 23: Scope of procedural measures
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. These measures shall be applied solely for the purpose of conducting specific, targeted criminal investigations or proceedings. 2. Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to: … (b) Other serious criminal offences committed by means of [a computer system] [an information and communications technology device]; and (c) The collection of evidence in electronic form ~~of any criminal offence~~ solely pertaining to the criminal offenses mentioned in clauses (a) and (b).

Our proposed amendment to Article 23(1) underscores the need to prevent potential misuse or overreach of procedural measures. The provision ensures that the powers conferred under this chapter are employed exclusively for specific and targeted criminal investigations or proceedings. As such, it reaffirms the commitment to uphold the principles of legality, necessity and proportionality in exercising these powers.

Our proposed amendment to Article 23(2) emphasizes that the powers and procedures should be applied only in cases of serious offenses committed by means of a computer system. It ensures that State Parties' resources are optimally utilized, prioritizing serious offenses that significantly impact public order, and avoiding its application to, for example, petty crimes.

With regard to our proposed amendment to Article 23(2), we recognize that the collection of electronic evidence is necessary to investigate and prosecute cybercrime and related offenses. However, we recommend that point (c) in Article 23(2) should be revised to narrow it to cases in points (a) and (b). In its current form, Article 23(2)(c) allows for the use of any investigatory power and procedure established by the Treaty for the prevention or detection of any offence. This not only widens the scope of the Treaty by going beyond the offences that the Treaty is meant to cover, but also raises compatibility issues with international human rights standards, such as necessity and proportionality It could potentially allow law enforcement authorities to use measures that seriously interfere with individuals' right to privacy or free expression to for example, prosecute petty offenses or criminal offenses, including content-related offenses, which are inherently inconsistent with States' human rights obligations.

By the same token, for our third amendment we recommend that the text of **Articles 29 and 30** should be edited as follows:

Article 29 (Real-time collection of traffic data)

1. With regard to the criminal offences established in accordance with articles 6 to 16 of this Convention, e ~~E~~*ach State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:*

Article 30 (Interception of content data)

1. Each State Party shall adopt such legislative and other measures as may be necessary, with regard to the criminal offences established in accordance with articles 6 to 16 of this Convention ~~*in relation to a range of serious criminal offences to be determined by domestic law*~~*, to empower its competent authorities to:*

2. Recommendation to further bolster the conditions and safeguards to which the powers and procedures established by the Convention are subject

Article 24 (Conditions and safeguards)

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 obligations under*~~ *international human rights law,* ~~*and which shall*~~ *incorporating at a minimum* ~~*incorporate*~~ *the principles of legality, necessity, proportionality, and necessitate a factual basis justifying access or application 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, a demonstrable grounds justifying access or 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.*

We recommend that Article 24(1) be amended to require that all States Parties provide in their domestic laws with effective protection of human rights, in compliance with international human rights law. The text should, explicitly and at a minimum, include not only the principle of proportionality but also the principles of legality and necessity. Likewise, the phrase "a factual basis justifying access or application of powers," emphasizes the need for a valid and substantiated rationale for establishing and applying the powers and procedures. The amendment aims to strengthen the safeguards and accountability in Article 24 by highlighting the importance of ensuring that any access or application of these measures is based on objective and verifiable facts, rather than arbitrary, biased or speculative reasons.

Respecting human rights is not only a legal obligation but also a practical necessity for law enforcement. Article 24(2) should also be amended to ensure prior judicial or independent authorization of the powers and procedures established by the Treaty. As the Office of the High Commissioner for Human Rights (OHCHR) underlined 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*."[4] Thus, "*respect[ing] for human rights [...] is a moral, legal, and ethical imperative [but also] a practical necessity for law enforcement*"[5] Indeed, the proposed amendment will ensure an impartial assessment of the necessity and justification for the application of such power or procedure.

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 international human rights law.[6] 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 to the legitimate aim pursued. Third, any independent (preferably judicial) authorization of surveillance powers should be prior to the exercise of those powers. This is to provide the necessary degree of independence and objectivity to prevent the abuse of surveillance powers. Such safeguard serves as an extra layer of protection to prevent potential abuses, enhancing accountability and upholding the rule of law. The "periodic disclosure of statistical data on the use of powers and procedures," also enhances transparency and accountability, making it mandatory for States Parties to periodically disclose statistical data on how they are using their powers. It ensures that states are not using their powers excessively or inappropriately, and allows for public scrutiny and debate, furthering democratic values.

As the European Court of Human Rights has repeatedly emphasized, the safeguard of prior judicial authorisation serves "*to limit the law-enforcement authorities' discretion,*" by establishing a practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case.[7] Regarding the grounds justifying application, we recommend removing 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. We also recommend the inclusion of adequate notification to ensure individuals are informed when their rights are affected by the powers and procedures outlined in this chapter. Notification allows individuals to exercise their rights, seek redress, and challenge any infringement on their privacy and other human

[4] 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

[5] Ibid.

[6] 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.

[7] ECtHR, *Szabó and Vissy v Hungary*, App No 37138/14, para 73.

rights. Access to effective remedies ensures that individuals have meaningful recourse when their rights are violated. [8]

3. Recommendation to require specificity

Article 26: Expedited preservation and partial disclosure of traffic data Each State Party shall adopt, in respect of traffic data that are to be preserved under the provisions of the article on the expedited preservation of stored [computer data] [digital information]**,** in relation to specified persons, such legislative and other measures as may be necessary to... Article 27: Production order (b) A service provider offering its services in the territory of the State Party to submit specified subscriber information relating to such services in that service provider's possession or control.

The existing language in Articles 26 and 27 may leave open a broader interpretation under which it would authorize orders or legal measures compelling retention of data related to all users of a service, even those who are not suspected of a crime and are not targets of a criminal investigation. While the language does not create an indiscriminate data-retention obligation, our recommendations aim to foreclose a potential broader interpretation. In particular, we recommend that Articles 26 and 27 be amended to ensure that any measures contained therein are directed against specific persons or unique identifiers. As the Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression highlighted, for surveillance laws to comply with international human rights standards, they must ensure that "*a surveillance operation be approved for use against **a specific person** only in accordance with international human rights law and when authorized by a competent, independent and impartial judicial body, with all appropriate limitations on time, manner, place and scope of the surveillance* (emphasis added)."[9]

[8] See UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020) and Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014), paragraph 40.

[9] UN Doc A/HRC/41/35, 28 May 2019.

4. Recommendation to limit the scope of preservation orders

Article 25. Expedited preservation of stored [computer data] [digital information]

2. Where a State Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored [computer data] [digital information] in the person's possession or control, the State Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that [computer data] [digital information], which are within the person's existing capability, for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A State Party may provide for such an order to be subsequently renewed.

Our amendments aim to clarify that service providers are not required to turn over data that they do not have access to, and that they are not required to change their products or services in order to access additional data for preservation purposes. They should not, for example, be required to remove or weaken the information security and privacy features of their products and services.[10]

5. Recommendation to remove search and seizure orders from the Convention

~~*Article 28. Search and seizure of stored [computer data] [digital information]*~~

~~4. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the [computer system] [information and communications technology device] in question, the information and telecommunications network, or their component parts, or measures applied to protect the [computer data] [digital information] therein, to provide, as is reasonable the necessary information to enable the undertaking of the measures referred to in paragraphs 1 to 3 of this article.~~

PI and EFF strongly recommend Article 28.4 be removed in its entirety. The language is too broad and can include disproportionate orders that can lead to forcing persons to disclose a vulnerability to the government that hasn't been fixed. It could also imply forcing people to disclose encryption keys such as signing keys on the basis that these are "the necessary information to enable" some form of surveillance.

[10] More recently, the United Nations General Assembly emphasized the importance of encryption for ensuring "the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association" in its 2022 Resolution on the Right to Privacy in the Digital Age (UN Doc A/RES/77/211).

Recommendations Related to Chapter V

6. Recommendation to limit the scope and to mandate dual criminality for international cooperation

Article 35. General principles of international cooperation
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, or for the collection, obtaining, preservation and sharing of evidence in electronic form of offences established in accordance with articles 6 to 16 of this Convention. ~~as well as of serious crime, including those offences covered by article 17 of this Convention when applicable.~~ This cooperation is, in all cases, contingent upon the principle of dual criminality being satisfied.
2. 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 the requesting State Party, ~~if the~~ provided that the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties. Absent the fulfillment of the principle of dual criminality, the relevant international cooperation request shall be considered invalid.

Our amendment to paragraph 1 prioritizes international cooperation in addressing universally recognized cybercrimes, as laid out in articles 6 to 16 of the Convention, and it is guided by the recognition that cybercrime laws should not unintentionally serve as a conduit for suppressing freedom of expression or other human rights. The amendment narrows the scope of cooperation to those offenses that are agreed upon under this treaty, thereby creating a clear framework for international cooperation. This not only reduces potential misuse of the treaty for matters that might infringe on internationally protected rights, such as free expression and association, but also respects jurisdictional differences and ensures that the principle of dual criminality remains a cornerstone of international cooperation under the Convention.

Our amendment to paragraph 2 ensures that international cooperation is strictly underpinned by the principle of dual criminality. The principle mandates that a conduct must be considered a criminal offense in both the requesting and the requested states for an international cooperation request to be valid. The principle of dual criminality provides a layer of protection for individuals, as it reduces the chance of states being able to request cooperation for offenses that are not universally recognized as criminal. By making dual criminality obligatory, the draft text now provides more clarity and predictability for State Parties in terms of their legal obligations under the draft treaty. If it was merely optional as currently written, this could create uncertainty and potentially lead to disputes between states. If dual criminality was optional, there might be a risk that states could seek cooperation in cases where the alleged conduct is not considered criminal in their own jurisdiction. This could potentially lead to the misuse of the treaty powers for political or other arbitrary purposes.

7. Recommendation to further bolster the protection of individuals' personal data in accordance with international human rights law

Article 36 (Protection of personal data)
1. A State Party transferring personal data pursuant to this Convention shall do so subject to the conditions of that State Party's domestic law and applicable international law**,** including international human rights law. States Parties shall not be required to transfer personal data in accordance with this Convention if it cannot be provided in compliance with their applicable laws concerning the protection of personal data and with minimum human rights-based data protection standards, such as the principles of lawful and fair processing, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. They may also seek to impose conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data. States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data.

PI and EFF welcome the revised wording of Article 36, noting particularly the effort to ensure that any data transfer is prohibited unless it is subject to both national and international data protection law safeguards. In addition, we suggest that the text of the Article be further amended to ensure that it includes explicit reference to international human rights law and standards. Data protection principles derived from existing international human rights law have been recognised in the Human Rights Committee General Comment on Article 17 of ICCPR[11] and the report of the UN High Commissioner for Human Rights on the right to privacy in the digital age.[12] Further resolutions of the General Assembly and the Human Rights Council on the right to privacy in the digital age have recommended the adoption of data protection legislation in accordance with international human rights law.[13]

[11] UN Human Rights Committee, General Comment No 16: Article 17, UN Doc HRI/GEN/1/Rev.1 at 21 (8 April 1988).

[12] Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).

[13] See for example, UN General Assembly resolution on the right to privacy in the digital age, UN Doc A/RES/77/211, para 7(i).

8. Recommendation to ensure 24/7 networks include secure and authenticated communications

Article 41. 24/7 network

1. Each State Party shall designate a point of contact available 24 hours a day, 7 days a week, in order to ensure the provision of immediate technical advise and assistance in identifying potential ~~for the purpose of investigations, prosecutions or judicial proceedings concerning~~ offences established in accordance with articles 6 to 16 of this Convention, and facilitating swift response to ongoing offenses covered by this Convention. ~~, or for the collection, obtaining, preservation and sharing of evidence in electronic form of offences established in accordance with articles 6 to 16 of this Convention, as well as of serious crime, including those offences covered by article 17 of this Convention when applicable~~.
2. The secretariat shall be notified of such point of contact and keep an updated register of points of contact designated for the purposes of this article.
3. Such assistance shall not include the collection, preservation or sharing of evidence. ~~facilitating or, if permitted by the domestic law and practice of the requested State Party, directly carrying out the following measures:~~

~~(a) The provision of technical advice;~~

~~(b) The preservation of stored [computer data] [digital information] pursuant to articles 42 and 43;~~

~~(c) The collection of evidence, the provision of legal information and the locating of suspects; or~~

~~(d) The provision of [computer data] [digital information] to avert an emergency.~~

4. A State Party's point of contact shall have the capacity to carry out communications with the point of contact of another State Party on an expedited basis. If the point of contact designated by a State Party is not part of that State Party's authority or authorities responsible for mutual legal assistance or extradition, the point of contact shall ensure that it is able to coordinate with that authority or those authorities on an expedited basis. To ensure the security of these expedited communications, encryption and authentication protocols shall be in place.

5. Each State Party shall ensure that trained and equipped personnel are available to ensure the operation of the 24/7 network with a focus on ensuring the security, reliability, and integrity of the network. All communications shall occur over secure and authenticated channels to safeguard the integrity and confidentiality of the information.

The scope of the proposed 24/7 network is very broad, covers a wide range of offenses, spans multiple stages of the legal process (investigation, prosecution, and judicial proceeding), and mandates a 24/7 availability. It also allows various forms of assistance and the need for expedited communication and collaboration between different States Parties' point of contact. Given its broad scope, implementing such provision could be resource-intensive for States' Parties. It's broad scope could also lead to overreach and potential misuse since it would allow for data to be collected, stored and shared freely across borders, bypassing the MLAT process and the respective conditions and safeguards, included in Articles 24 and 36. Finally, while 24/7 networks may also play a role in later stages of the legal process (prosecution and judicial proceedings), its primary focus is typically on the initial investigation stage due to the unique time-sensitive and global nature of cybercrime. Therefore, we suggest making this article narrower in scope.

First, it should focus only on specific criminal investigations. Second, it should clarify the role of the point of contact to limit it to its technical advice, assisting in identifying potential offenses, and facilitating swift response to ongoing crimes. However, it should be clear that the point of contact should not be responsible for the collection, preservation or sharing of evidence since such exchange could bypass the safeguards included in the MLATs and in article 24 and 36 of the present Convention.

Additionally, our proposed amendment to Article 41 seeks to bolster the security, reliability, and integrity of 24/7 networks by implementing security and authentication methods. Safeguarding communication between States Parties is paramount to protect data, prevent unauthorized access or misuse, and mitigate potential threats of hacking and espionage. Cross-border cooperation mechanisms can create new privacy and information security risks where requests are fraudulent or not properly authenticated, or where information is delivered over an insecure channel and intercepted by unauthorized third parties. We recommend the adoption of security, encryption, and authentication mechanisms for the delivery of requests and responses. If they are optional, and especially if they are agreed upon bilaterally and on a case-by-case basis, the likeliest outcome will be the frequent use of unencrypted and unauthenticated channels. This would allow, for example, a malicious actor to impersonate a public authority in another State in order to improperly access a target's personal data with a counterfeit request. Hence, the amendments serve to maintain the integrity of the treaty's enforcement and uphold the confidence of States Parties in the integrity of the international cooperation mechanism.

9. Recommendation for enhancing data protection in law enforcement cooperation to close open-ended scenarios

Article 47. Law enforcement cooperation

1.States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, and in conformance with Articles 23(1) and 24 to enhance the effectiveness of law enforcement action to combat the offences covered in Article 6 to 16 of this Convention. States Parties shall, in particular, take effective measures:

(a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

~~(b) To cooperate with other States Parties in conducting inquiries with respect to offences covered by this Convention concerning:~~

~~(i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;~~

~~(ii) The movement of proceeds of crime or property derived from the commission of such offences;~~

~~(iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;~~

~~(c) To provide, where appropriate, necessary items or data for analytical or investigative purposes. ;;~~

(d) To exchange, where appropriate, non-evidentiary information with other States Parties concerning specific means and methods used to commit the offences covered by this Convention, including the use of false identities, forged, altered or false documents and other means of concealing activities, as well as [cybercrime] tactics, techniques and procedures [associated with the use of information and communications technologies for criminal purposes];

[…]

~~(f)To exchange information and coordinate administrative and other measures taken, as appropriate, for the purpose of early identification of the offences covered by this Convention.~~

2.With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them to ensure they are aligned with international human rights law and data protection principles, including Article 24 and 36 of this Convention. In the absence of such agreements or arrangements between the States Parties concerned, the States Parties may consider this Convention to be the basis for mutual law enforcement cooperation in respect of the offences in Article 6 to 16 of ~~covered by~~ this Convention, including the safeguards embedded in Article 24 and 36. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies

PI and EFF believe that any law enforcement cooperation to investigate and prevent cybercrime must respect and uphold universally recognized human rights. The current wording of this Article risks

supporting open-ended law enforcement cooperation without detailing the limitation and safeguards required under international human rights law. The amendment to the first paragraph seeks to limit the scope of this cooperation to universally agreed crimes that are the object of this Convention (Article 6-16), and to ensure that domestic law is in conformance with international human rights law, as well, as the safeguards embedded in the present Convention Article 23(1) and 24.

The subsequent amendment proposes the removal of Article 47(1)(b)(c) and (f) from the proposed Treaty, aiming to prevent States Parties to share personal data in ways that bypass the safeguards embedded in the Mutual Legal Assistance framework. States should not leverage the Treaty to authorize or require personal information sharing outside the bounds of the existing mutual legal assistance treaty, the safeguards established under the MLA, and the MLA vetting mechanism. Such safeguards should not be removed without providing comparable protections and limitations, and their removal invites misuse of the mutual legal assistance framework for transnational repression. In this respect, we note that under the current proposal, Article 24 does not apply to the international cooperation chapter, and the current wording of Article 36 does not specify the minimum data protection principles, therefore the protection afforded to sharing of personal data under this Article is insufficient. Moreover, the data in question has the potential to reveal the location of an asylum seeker or political dissidents, inviting misuse of the criminal mutual legal assistance framework for transnational repression.

The final amendment in paragraph 2 ensures that the scope is limited to Article 6-16 of the present Convention, and the need to apply the conditions and safeguards under Article 23(1) and 24 to this chapter. This serves as a crucial condition for any law enforcement cooperation, ensuring that respect for privacy and data protection is inherent in all international cooperative efforts.

Recommendations related to Chapter VII technical assistance and information exchange

10. Recommendation to ensure that any assistance provided to State Parties does not result in human rights violations

Article 54. Technical assistance and capacity-building
1. States Parties shall, according to their capacity, consider affording one another the widest measure of technical assistance and capacity-building, including training and other forms of assistance, the mutual exchange of relevant experience and specialized knowledge and, where possible, the transfer of technology on mutually agreed terms, with a view to facilitating the prevention, detection, investigation and prosecution of the offences covered by this Convention. States Parties shall ensure that any technical assistance and capacity building is conditional upon prior human rights impact assessments that take into account the capacities of the technologies at issue as well as the situation in the recipient State, including compliance with human rights, adherence to the rule of law, the existence and effective enforcement of applicable laws regulating surveillance activities and the existence of independent oversight mechanisms.

We recommend that Article 54 (technical assistance and capacity-building), which requires state parties to provide assistance, including, *inter alia*, capacity building, training and equipment transfers, to one another, is amended to ensure that no such activity takes place in absence of a prior human rights risk and impact assessment.

Indeed, the risks associated with assisting states in deploying and using extremely intrusive surveillance capabilities to the authorities of other countries are not new.[14] However, in light of recent reports on the misuse of certain surveillance technologies by several states, UN Special Rapporteurs, the High Commissioner for Human Rights and other independent experts have called for the adoption of control regimes applicable to surveillance technologies, including requiring "*transparent human rights impact assessments that take into account the capacities of the technologies at issue as well as the situation in the recipient State, including compliance with human rights, adherence to the rule of law, the existence and effective enforcement of applicable laws regulating surveillance activities and the existence of independent oversight mechanisms.*"[15]

Within the European Union, the European Ombudsperson noted during her inquiry into whether the European Commission assessed human rights impacts before providing support to African countries to develop surveillance capabilities, activities are often "*implemented in countries with major governance issues and, in many cases, with poor human rights records. This increases the risk of human rights violations... If the surveillance technologies and capacity transferred are used by the partner countries for purposes not foreseen under the project, there is a risk for human rights of individuals in these countries, as well as for the ability of the EU to fulfill or realize its human rights obligations.*"[16] Consequently, in her decision dated 28 November 2022, the European Ombudsperson recommended that the Commission now require that an "*assessment of the potential human rights impact of projects be presented together with corresponding mitigation measures*" and concluded that the lack of such protections constitutes a

[14] PI, Challenging the Drivers of Surveillance, https://privacyinternational.org/challenging-drivers-surveillance

[15] UN High Commissioner for Human Rights, report on the right to privacy in the digital age, A/HRC/51/17, paragraph 56.

[16] Decision on how the EC assessed the human rights impact before providing support to African countries to develop surveillance capabilities (case 1904/2021/MHZ), para 25, https://www.ombudsman.europa.eu/en/decision/en/163491

"*serious shortcoming*" and poses a clear risk that these surveillance transfers might cause serious violations of or interferences with other fundamental rights.[17]

Furthermore, in its Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of EU law in relation to the use of Pegasus and equivalent surveillance spyware, the European Parliament called on the European Commission and the European External Action Service (EEAS) "*to implement more rigorous control mechanisms to ensure that... the donation of surveillance technology and training in the deployment of surveillance software, does not fund or facilitate tools and activities that could impinge on the principles of democracy, good governance, the rule of law and respect for human rights.*"[18] The Recommendation of the European Parliament also underlines the need to "*include in every human and fundamental rights impact assessment a monitoring procedure on the potential abuse of surveillance*" by non-EU countries.[19]

[17] Ibid.

[18] European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)), para 96, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html.

[19] Ibid, para 97.