Statement to the Second Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering ICTs for Criminal Purposes
June 7th, 2022

On item #5: General Provisions

Madam Chair, thanks for allowing the Electronic Frontier Foundation to take the floor. We would like to share our appreciation for the efforts made by the Ad Hoc Committee, its Secretariat, and staffers to facilitate the current discussions.

EFF would like to provide comments on the section of "**General Provisions",** focusing on the importance of having a human-rights-by-design approach in the proposed Cybercrime treaty. We are heartened to hear several Member States recalling their duties to ensure that the proposed Convention should be in line with their international human rights obligations.

On Q.3, EFF believes that the powers and procedures should be limited in scope to specific criminal investigations or proceedings of the criminal offenses established in the criminalization chapter of the proposed Convention. Such limitation is necessary to ensure that the powers and procedures are not 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. Its procedural measures should similarly be limited to addressing cybercrime, not the full range of criminal conduct.

On Q.5, Any proposed cybercrime treaty should always be in line with States' applicable human rights obligations. We welcome the suggestion made by some Member States to add to the preamble a recognition of its international human rights commitments and to include a general clause calling for the protection of media freedom, journalists, and whistleblowers.

On Q.6, We support Member States' suggestions on first agreeing on the substantive measures and then returning to definitions.

On Item #6: Criminal Procedural Measures

Madam Chair, thanks for allowing the Electronic Frontier Foundation to take the floor. We would like to share our appreciation for the efforts made by the Ad Hoc Committee, its Secretariat, and staffers to facilitate the current discussions.

Q. 4 What is the scope of the chapter on procedural measures and law enforcement? Should it apply only to the list of offenses established by the convention (in its chapter on criminalization)? Could it also apply to other offenses? Why would such enlargement to other offenses be necessary?

The powers and procedures should be carefully scoped so that they apply to the criminal offenses established in the criminalization section of the proposed Convention. Such limitation is necessary to ensure that the powers and procedures are not being used for less serious crimes or crimes that may not be consistent with States' human rights obligations.

Moreover, as we have noted in previous comments, the proposed Convention is about addressing cybercrime, not a general-purpose law enforcement treaty. Thus, its procedural measures should similarly be limited to addressing cybercrime, not the full range of criminal conduct.

Q. 5. Which conditions and safeguards should procedural measures be subject to?

We believe that any proposed obligations to enable the investigation and prosecution of a specific crime should come with robust human rights safeguards. Thus, we recommend that any future agreement apply conditions and safeguards to every procedural measure. International human rights law provides that monitoring, collection, retention, access, and sharing is an interference with the right to privacy, and hence, the permissible limitation test to the right to privacy should be applied: legality, legitimate aim, necessity, and proportionality.

Robust and accessible redress and transparency mechanisms are also critical.

Q. 6. Should there be also a reference to universal legal principles (e.g., necessity, proportionality), and which ones could be agreed upon?

The draft Convention should explicitly indicate that any interference with human rights must respect the principles of legality, necessity, and proportionality. This includes any interference with the right to privacy and data protection.

Moreover, human rights protections should not be optional and should not defer to case-by-case agreements to define how people will be protected against potential abuses or misuses of investigatory powers. It should also avoid barriers that would prevent states from adopting stronger human rights protections.

Second Group of Questions

Q.1 Which powers and procedures should the convention foresee for the purposes of detecting, disrupting, investigating, prosecuting, and adjudicating the concerned offenses?

As we have noted in previous comments, the draft Convention should remain focused on law enforcement. Its procedural measures and investigative powers should, therefore, focus on the investigation and prosecution of specific crimes as defined in the chapter on criminalization.

We, therefore, recommend the inclusion of a provision comparable to Article 14(1) of the Budapest Convention, which states:

> Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

Any such powers and procedures need to be compliant with existing states' obligations under international human rights law.

Q.2. Are there any specific conditions and safeguards that should apply to certain procedural measures?

Parties should categorically reject any generalized and indiscriminate data retention obligation. Such measures are inherently an unnecessary and disproportionate measure.

The proposed Convention should require prior independent judicial authorization as a condition for exercising the investigative powers it adopts, with the exception of genuine emergency measures.

While robust safeguards such as a strong showing of grounds and prior judicial authorization should be a precondition to state access to all types of communications-related personal data, real-time collection, real-time disclosure, and interception should only be available upon an additional showing of investigative necessity.

The treaty should prohibit the use of any procedural powers in a manner that would undermine or interfere with the use of encryption.

Transparency obligations should apply to the investigative powers adopted in this treaty. Parties should, at minimum, be obligated to report annually and publicly on how frequently these powers are exercised,

how many individuals and accounts were impacted, what crimes justified the exercise of these investigative powers, and how frequently exercise of these powers resulted in a criminal conviction.

There should be strict and explicit limits on any confidentiality mechanisms that accompany the investigative powers in this treaty. Confidentiality can only be justified where strictly and demonstrably necessary to avoid placing an investigation in jeopardy.

Independent regulators should also be empowered to scrutinize the exercise of the treaty's investigative powers and to issue binding remedies where these powers are not exercised in a manner that is necessary and proportionate, as well as of any invocation of confidentiality. Core immunities and privileges should be explicitly safeguarded.

Q. 3. Should certain procedural measures apply to certain types of data?

While it is acceptable to adopt different procedural mechanisms for different types of data (e.g. different preservation periods, expedited response times), it is not acceptable to allow for access to subscriber data or metadata with fewer safeguards in place, as these categories of data can be as revealing as content data or more so, as noted by numerous UN resolutions on the right to privacy in the digital age, as well as independent human rights experts and regional courts. Access to these types of data must be premised on a strong showing of reasonable suspicion and subject to prior judicial authorization.

Q.4. What time limits should apply to the preservation of data pending a request by competent authorities for its disclosure?

Preservation orders should explicitly be limited in each instance to as long as they are necessary for competent authorities to seek disclosure and, moreover, should expire after no longer than 90 days, subject to renewal by an independent judicial authority.

Q.5. What is the difference between electronic information vs. computer data; accumulated v. stored (data or information)?

Any processing of personal data (including access, retention, analysis, etc) should be subject to limitations and safeguards in line with data protection principles.

Q.7 Should the suspicion of ICT-related crimes or the commission of criminal offenses be stated as grounds for search and seizure or for interception of content data? The availability of all investigative powers under this proposed Treaty should be explicitly premised on a strong, objective, and individualized reasonable suspicion showing that the use of the power in question will yield evidence of a specific offense.