Sixth Session of the Ad Hoc Committee

Submission on the Draft Text of the Convention on Cybercrime

AUGUST 2023

Preamble

The Internet Society is a global nonprofit organization empowering people to keep the Internet a force for good: open, globally connected, secure and trustworthy. We support and promote the development of the Internet as a global technical infrastructure and a resource to enrich people's lives. Our work focuses on: advancing the development and application of Internet infrastructure, technologies, and open standards; advocating for policy that is consistent with our view of the Internet; and building and supporting the communities that make the Internet work.

The Internet Society has contributed to the Ad Hoc Committee's work since its initiation and is pleased to see that the Consolidated Negotiating Document (CND) is focused on areas where there is consensus, and has been made available to stakeholders for comment, reflecting the importance of strengthening cooperation among States and stakeholders. We appreciate the opportunity to offer the following comments on the CND:

Chapter I. General Provisions

Article 1: Statement of purpose

We recommend that the Convention clearly and narrowly defines the scope of the Convention. We do not support the use of the term "the use of informational and communication technology for criminal purposes". We prefer the term "cybercrime", which is recognized in other international and regional instruments such as the Council of Europe Cybercrime Convention. Further, it should be limited to serious criminal offenses.

Article 2(e): Use of terms

We consider that the definition of service provider is overly broad. For instance, it may unintentionally include e-government and other services that are not intended to be covered by this Convention. Additionally, we would like to see the definition focus on the applications and services that utilize transportation technologies such as the Internet, rather than Internet infrastructure services on which

those services operate, recognizing the incidental nature of those services, by way of an input, to the applications and services that are used to commit serious cyber criminal offense

Chapter II. Criminalization

Articles 6-10

We are concerned that security and privacy researchers may be at risk of criminal charges and sanctions as a result of these broadly proposed provisions. They may be deterred from fulfilling their important public interest role of voluntarily investigating, detecting, reporting, and mitigating vulnerabilities to the benefit of Internet-users all over the world. We believe this Convention should explicitly provide legal protections for these technical experts beyond the protections in Article 10.

Article 11: Computer-related forgery

It is well known that some services seek personal data from their users even when that data is not needed to provide the service. In some cases, the users cannot use a service without completing the mandatory fields, such as "date of birth". Personal data could be used for identity theft or account takeover, if there is a data breach. So, where users provide incorrect information to protect their personal data, that should not be criminalized. We recommend that this article be clarified to ensure that users in these and similar circumstances are not criminalized.

Article 13: Offenses related to online child sexual abuse or child sexual exploitation material

The legislative and other measures that may be necessary to establish offenses related to online child sexual abuse or child sexual exploitation material under members' domestic law, must not prevent, obstruct or otherwise undermine the use of end-to-end encryption or its users' expectations of privacy and security.

Chapter IV Procedural measures and law enforcement

Article 23: Scope of procedural measures

We agree with Privacy International and EFF that such measures must only be applied solely for the purpose of conducting specific, targeted criminal investigations or proceedings regarding serious crimes.

Article 24: Conditions and safeguards

We support the proposed amendments by Privacy International and EFF to strengthen the safeguards for the powers and procedures.

Article 25: Scope of preservation orders

It is important that the article be amended to clarify that service providers cannot not be required to build or add new capabilities to store data as that could introduce new security vulnerabilities or other weaknesses in their systems.

Article 26: Expedited preservation and partial disclosure of traffic data

To reduce the potential harm to innocent and legitimate users, we support the proposed amendments by Privacy International and EFF to require these powers and procedures be applied to specified persons.

Article 29: Search and seizure

As Privacy International, EFF and Global Partners Digital point out, this broadly worded power could be used to cause disclosure of security knowledge and assets such as encryption keys which could harm security for all users.

Articles 29 and 30: Real time collection and interception of content data

We further agree with Privacy International and EFF that given the invasive nature of these powers, they should be confined to the criminal offenses established under articles 6 through 16. Further, Article 30(2) should be clarified to ensure that service providers are not required to disable or circumvent end-to-end encryption on their services.

Finally, we strongly recommend that member states incorporate the guidance Privacy International, EFF, and Global Partners Digital, three non-profit organizations with specific expertise in privacy and other fundamental rights and values, concerning the protection of personal data and the rights of users.