The Electronic Frontier Foundation would like to signal its continued appreciation for the opportunity to provide input into the development of this Convention. We want to thank the Secretariat for promoting inclusive multi-stakeholder participation in the global or regional debate on e-evidence and cybercrime.

Today, our remarks focus on the proposed offenses in Clusters 5 and 7.

For each of these clusters, we restate our previous objection that content crimes are not a proper subject for this treaty.

Should these topics nevertheless remain in the Treaty, we note our concerns with the following:

Cluster 5:

- Given that these provisions are specific to the use of a computer or information and communications technology, they potentially apply numerous deep "stacks" of online services **commonly used in any online transmission of information**. Any criminal law provision so focused should thus carefully consider how deep into the stack its application is attended and use precise terms to limit imposing liability on those removed from the actual wrongdoing. The law must be precise in its terms both as to what acts violate the law and what acts involved in the provision of computer services are intended to be covered.
    - The term "facilitating," as used in proposed Articles 18(1)(b) and 19(1), is vague and can subject those with attenuated connections to the primary offenders to threats of liability, thus risking the chilling of protected expression, sexual and otherwise.
    - We agree with removing "participating in … any business," as used in Article 18(1)(g), but the "related to" is similarly vague and could lead to attenuated liability far down the stack.

We welcome the deletion of "or has reasons to believe" .. such amendment addressed our concerns regarding the elements of intent.

- Article 18(5) acknowledges that some states exclude from their definition of CSAM materials that did not involve the exploitation of an actual child in their creation, such as non-filmed artistic renderings and computer-generated images, and thus permits states not to apply 18(2)(b) and (c). But 18(2) nevertheless includes "drawings" and "written material" among potentially offending media. We support State's recommendations to exclude such media.
- Article 20(3) contains a provision that eliminates liability if "a person has taken reasonable steps to ascertain that the person is not a child."
    - It is unclear whether this requires prosecutors to establish the absence of age verification or whether it merely, and insufficiently, creates an available affirmative defense that the defendants would have to establish. The latter is insufficient to protect freedom of expression.

**Cluster 7**

- We recommend keeping the provision of Article 25(3), since is important for protecting human rights, including the right to disseminate newsworthy information and other

matters of public importance. The provision might benefit from specifying some examples of legitimate purposes without limiting the clause's breadth.

Madame Chair, we've kindly submitted a detailed analysis in written form, for Articles 6, 7, 8, and 10 of Cluster 1 and Arts. 11, 12, 13 & 14 in Cluster 2, we hope it could be published on the ad hoc committee site. In our submission, we recommend:

First, add a requirement of unauthorized intrusion onto networks or devices and define it as criminalizing conduct that results from bypassing technical security safeguards.

Second, require that prohibited conduct be fraudulent intent and results in 'harm'. However, such harm, for example, loss and damage should be limited to impairment to a computer or data and the costs of responding to those harms, respectively.

Third, include a public interest defense, but let domestic law define it in terms of what public interest evolves over time.

Due to the technical complexity of this topic and the evolution of technology over time, let me illustrate the need for such amendments by sharing a few specific scenarios.

These provisions risk criminalizing the work of security or social researchers, even when they monitor publicly available information over the internet **since no technical security safeguards need to be bypassed** and **no fraudulent or dishonest intent is required to** violate a TOS. Websites could effectively criminalize scrutiny of their services by publishing terms of use that forbid its access.

For example, social researchers have developed tools to better document the targeting of advertisements on social media platforms. These tools provide important contributions to the public discourse but are understandably sometimes objected to by social media companies who are the object of their critiques. Yet these tools operate by intentionally copying and downloading digital information and could be viewed as interfering with computer systems. Should a company prohibit a tool of this type in its terms of use, the resulting research could be viewed as ''without right', or 'without authorization'.

Let me share another example of why these changes are needed. Companies, for example, can transform their terms of use into criminally enforced anti-competitive prohibitions. For example, a social media company might prohibit the use of a 'plugin' that allows users to aggregate messages from the platform alongside messages from competing platforms in one place. The tool would be highly convenient for end users who enjoy multiple services but are objectionable to the platforms themselves. Yet resolving these disagreements should not be a question of criminal liability but, if anything, a breach of contract, as there is no fraudulent intent on the part of the tool's creators, and the data export capabilities of the tool may be in the public interest.

The proposed Convention should ensure that these provisions are not criminal in nature. Therefore, a provision protecting public interest should be included, and liability should be qualified as requiring infringement on security safeguards and fraudulent intent.