Electronic Frontier Foundation Oral Statement Cluster 5, 1 and 2
Delivered by Katitza Rodriguez
January 16, 2023

Thank you, Madame Chair. Today, our remarks focus on the proposed offenses in Clusters 5 and Clusters, 1 and 2. For each of these clusters, we have shared proposed detailed amendments in written form, for publication and distribution to Member States. 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 provisions should be precise in terms of 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.
    - We agree with removing "participating in … any business," as used in Article 18(1)(g), but the new term "related to" is similarly vague and could lead to attenuated liability far down the stack.
- The intent elements must be clarified so that it is clear that one does not commit the offense unless they have the specific intent to produce, possess or disseminate child sexual abuse material, rather than merely intend to provide online services.
    - The constructive knowledge standard in Art. 18(10(g), "Participating in or receiving profits from any business that the person knows or has reasons to believe is related to any child sexual abuse or exploitation material," is insufficient, and at a minimum should have a subjective element, such as "reckless disregard of a known serious risk."
    - We welcome the deletion of "or has reasons to believe" on the new version CND.. 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. It thus permits states not to apply 18(2)(b) and (c). But 18(2) nevertheless includes "drawings" and "written material" among potentially offending 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 free expression and the right to a fair trial.

On Cluster 1 and 2, Madame Chair, we support the proposed amendments from Red en Defensa de los Derechos Digitales, and Derechos Digitales presented on Friday. Due to the technical complexity of this topic, let me illustrate the need for such amendments with two examples.

Social researchers have better developed tools to document advertisements' targeting 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.