Third Prepared Remarks of EFF Policy Director for Global Privacy Katitza Rodriguez
Groups 15: Article 41. 24/7 network; **Article 47**. Law enforcement cooperation.
Article 28(4): Search and Seizures.

August 30, 2023

Thank you Madame Chair,

Speaking on behalf of EFF, a non-profit organization with over 30,000 members across 86 countries. My intervention today will focus primarily on Article 41 and 47.

Scope and a lack of safeguards continue to remain a central challenge for the international cooperation chapter as a whole and particularly for Articles 41 and 47. As currently drafted, Articles 41 and 47 are **not constrained** by important safeguards such as those in Article 24 and seem to authorize direct sharing of personal and even highly sensitive data *(safeguards problem)*. Both Articles also apply to **any serious offense** without being constrained by **any dual criminality obligation** *(broader scope of assistance problem*). Direct cooperation under these Articles also does not require assessment by States' central authorities as would otherwise be required by Article 40(12), and it is not clear to what extent the grounds of refusal in Article 40(21) are engaged as it does not appear that any formal **request** for mutual legal assistance is required for any direct cooperation that occurs under Articles 41 and 47 (*no MLA request, MLA safeguards problem*).

Recent proposals to evolve Article 17 and expand the scope of Chapter V beyond serious crimes **do not address these problems.**

Problem 1: Article 47(1)(c), which demands State Parties' close cooperation, particularly in providing "necessary items or data for analytical or investigative purposes." However, it lacks

specificity, disconnected from **specific** criminal investigations or proceedings. This omission raises alarms, especially as there's **no exclusion** for sharing "personal data," including sensitive

biometric, traffic, and location data and no requirement that information sharing be proportionate and incorporate proper safeguards. These sensitive pieces of information must be held to effective data protection and privacy safeguards. The article **requires urgent revision to align with these** protections and to align to a **specific criminal investigation**. Without these revisions, it opens doors to **sharing massive databases and AI training data sets**, putting human rights at risk. Biometric data, face and voice recognition, have been abused in some countries against protesters, minorities, journalists, and migrants. The convention should not provide an opportunity to escalate these dangerous patterns beyond borders.

Problem 2:

The open-ended scope of Chapter V also risks undermining law enforcement cooperation on actual cybercrime offenses by diluting resources. Contrary to other treaties, Chapter V also is not limited to assistance in relation to investigations, prosecutions and judicial proceedings (UNCAC, Article 46; Budapest second additional protocol, Article 2) or to situations where there is a reasonable suspicion that legal assistance will produce evidence of an offense (UNTOC, Article 18). As a result, States will be obligated to provide assistance in relation to a vast array of crimes that have no connection to the objects of this Draft Convention.

The 24/7 network, for example, is intended to process urgent requests with more immediacy. Requiring states to provide immediate assistance on evidence gathering in respect of any and all serious crimes would either greatly dilute the ability of this network to respond with immediacy or, alternatively, would be extremely or even prohibitively resource intensive for State Parties. To the degree States decide to

involve central authorities in overseeing mutual legal assistance that occurs through Articles 41 and 47, requiring cooperation in relation to all serious offenses also risks overwhelming these bodies.

Problem 3:

The broad scope of Chapter V means that **Articles 41 and 47 could also lead to overreach** and misuse, particularly in the **absence of a dual criminality requirement** and the requirement to involve central authorities in the provision of immediate assistance. Under Articles 41 and 47, States are authorized to cooperate directly, without any requirement to consult a States' central authorities. Unfortunately, many offenses that would meet the "serious crimes" threshold criminalize conduct that is protected by human rights. ***In practice,*** *point of contacts will be obliged to* assess numerous offenses from multiple jurisdictions and to understand the relation [**or legality]** of these offenses to their national legal system. Expertise for assessing foreign offenses are legitimate, consistent with States' human rights obligations, and in line with national law is typically housed in States' central authorities.

The requirement to assess assistance scenarios quickly (Article 41), in relation to a vastly expanded range of offenses, and without requiring involvement of central authorities greatly multiplies the risk of human rights violations in global cooperation.

Therefore, we recommend to narrow the scope of mandatory cooperation through the 24*7 network to cover immediate technical advice and assistance in identifying potential offenses under Article 6-10 and that sub-Articles 41(1) and (3) be amended accordingly. We also recommend that the most intrusive elements of Article 47 be deleted, namely paragraphs 47(1)(b), (c) and (f).

In conclusion: The Convention should not 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: The Central Authority. Such safeguards should not be removed without providing comparable protections and limitations, as their removal invites misuse of the mutual legal assistance framework for transnational abuse.

Analysis on Article 28(4) - we propose deletion of the entire paragraph 4.

Article 28(4) makes it possible for states to order "*any person who has special knowledge*" of a particular computer system to provide the necessary information to search that computer

system. Article 28.4 is one of the most alarming provisions under consideration, which we sincerely hope does not make the final cut. This article raises serious concerns about individual rights, as it leaves room for interpretation that might force someone with knowledge, for example, an engineer, to involuntarily assist in breaking security measures or reveal an unpatched vulnerability to authorities. There's also an implicit threat of obliging engineers to hand over encryption keys, including signing keys, under the guise that they provide 'necessary information' for surveillance purposes. Article 28.4 hinting at the possibility of compelling individuals to relinquish encryption keys, thereby endangering both personal and wider digital security. Such a provision could potentially enable states to compel engineers to bypass established corporate policies, pressuring individual employees into revealing confidential data. This order not only could breach corporate procedures but also erodes trust in organizational operations.

In summary, in the absence of independent oversight and due process safeguards, such provision runs the risk of being abused to compel, for example, an IT engineer, traveling company or government employee with special knowledge of an ICT system to provide assistance in subverting technical access controls such as access credentials, encryption, and just-in-time approvals, thereby allowing data exfiltration without the knowledge of the responsible data custodian. Such provision could not only expose individual employees, such as traveling employees of IT companies or even government employees to coercion and criminal prosecution but could also undermine cybersecurity of ICT products and services more broadly. Instead, the convention should ensure that a data custodian (i.e. a legal person) and its executive officers are responsible for processing data access requests.

The ability to compel individuals rather than legal persons can exacerbate the problem. For example, adding the word "legal" in front of persons may not be adequate and could in fact encourage some states to hire private sector actors (cyber mercenaries) to hack into secure systems to exfiltrate data.

Finally, the scoping of this provision differs in substance from the Budapest Convention (BC) and is much broader. In BC, this provision only applies to para 1 and 2 of Article 19 (search and

seizure). In this draft, it applies more expansively to para 2 and 3 of Article 28 (Search and seizure). Paragraph 3 of Article 28 includes the most intrusive and extreme measures of this

provision, including seizure, making copies, deletion or rendering content inaccessible. For all these reasons, we recommend deletion rather than redrafting.

Thank you for your attention.