Second Prepared Remarks of EFF Policy Director for Global Privacy Katitza Rodriguez
Groups 5, 10, 11, and 15

August 29, 2023

Thank you Madame Chair.

We strongly endorse Privacy International and Global Partners Digital's observations on safeguards on privacy and data protection, particularly in light of the current unprecedented scope of the Convention and its lack of adequate safeguards.

We support the amendment in paragraph 2 of Article 24, which introduces the right to an effective remedy. But the efficacy of such a right hinges on the user's knowledge of and ability to challenge disproportionate or arbitrary data demands. If a person isn't notified about a demand for their data, of course they cannot seek a remedy, putting their basic privacy and due process rights at risk. Article 24 needs a notification requirement and should compel States to publish statistical information periodically detailing the use of powers, procedures, and remedial actions taken.

Because strong safeguards are lacking, we support replacing "shall" with "may" in paragraph one of Articles 35, 40, 45, 46, and 47. Article 40(4) allows a State's competent authority to proactively share information linked to criminal matters without an initial request if it's perceived to be beneficial for another state's criminal processes. Such "information" which is still undefined in article 2, likely includes personal data and could encompass information gathered from wiretaps, device scans, or even indirect investigative leads. Nothing in the provision limits the scope or specifies targets for the information shared.. The lack of limitations and specific definitions needs to be remedied.

Article 47(1)(c) outlines the requirement for State Parties to engage in close cooperation, specifically focusing on the provision of "necessary items or data for analytical or investigative purposes'' when deemed suitable. This provision lacks precision, as again, it isn't linked to specific criminal investigations or proceedings. Additionally, nothing in this provision excludes the sharing of "personal data," including biometric data, "traffic data," or other categories like location data, all of which are sensitive and intrusive information that should be subject to robust safeguards. The Article needs to be revised to add these protections as well as requirement that it is linked to a specific investigation.

Without these revisions, the provision opens the door to cross-border law enforcement sharing of massive biometric databases or artificial intelligence training datasets, endangering human rights everywhere. Biometric data, facial recognition and voice recognition systems have been used in various countries to identify, surveil, and prosecute protesters, minorities, migrants, human rights defenders, journalists, and opposition leaders. The convention should not provide an opportunity to escalate these dangerous patterns beyond borders. 47(1)(c) therefore raises similar concerns to Article 40(4), granting a State the ability to share "information relating to criminal matters" without the need of a formal request.

Thank you for your attention.

=