Privacy International's Oral Statement to the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes:

Agenda item 6 - Provisions on procedural measures and law enforcement

As delivered by Ioannis Kouvakas on 18 January 2023

Thank you, Chair, for giving Privacy International the opportunity to take the floor during this session.

As stated in our written submission before the Ad Hoc Committee, while we are not convinced whether a global cybercrime treaty is really necessary, it is fundamental that any instrument which is eventually adopted has human rights at its heart.

Our intervention today focuses on Articles 41 & 46(4).

With respect to Article 41:
Widening the scope of all crimes committed with the use of ICT significantly risks undermining human rights, including the right to privacy and the right to a fair trial. We recommend that the scope of procedural measures is limited to the investigation of the criminal offenses outlined in the Convention. It should further be limited to offenses that are encoded in national law as serious crimes. As the 2022 UN Security Council's Counter-Terrorism Committee Executive Directorate noted, in attempting "to address law enforcement's jurisdictional problems, the substantive law will become weakened, giving law enforcement too-quick access with too-little due process".

We therefore suggest that **Art 41(2) is amended to remove points (a) and (b). Moreover, point c should be amended as follows: "the collection of evidence in electronic form of serious [offences set forth in this Convention]".**

With respect to Article 46:
Paragraph 4 seeks to compel persons with special knowledge to provide technical assistance, which could include compelling security experts to disclose vulnerabilities of specific software or to force companies to provide relevant authorities with access to encrypted communications.

We strongly recommend removing Article 46(4).

As more people's lives are lived in the digital realm, communication security tools, such as E2EE, are increasingly important to the protection of human rights, including the right to privacy.

Imagine authorities are authorized to compel experts to exploit security flaws. In that case, authorities will more likely be incentivized to build an "arsenal" of security vulnerabilities to attack a target in the event of a criminal investigation. This interest, in turn, will discourage authorities from notifying the affected provider, with the view of fixing the software vulnerability that has been discovered. If such a vulnerability is fixed, authorities will not be able to exploit the system.

In other words, patching or fixing vulnerabilities is critical to protecting billions of people across the globe.

Thank you, Chair.