EFF's Oral Intervention

Delivered by George Wong

Written by Katitza Rodriguez

29 August to 9 September 2022, New York

EFF would like to thank the Chairwoman, the Secretariat, and staffers for the critical work facilitating this process.

On Questions 1, 2, and 4:

The international cooperation components of the Convention should only be limited in scope to investigations or prosecutions of specific crimes itemized in the Convention and to the collection of electronic evidence for criminal offenses outlined in the substantive portions of the Convention or to a finite list of serious criminal offenses explicitly itemized and defined in the Convention. The Convention should explicitly define serious crime as an offense punishable by a maximum deprivation of liberty of at least four years or a more severe penalty.

The international cooperation chapter should also include a dual criminality mechanism and should never include an open-ended scope that applies to every type of crime. A *de minimis* clause should also be adopted as a ground of refusal to allow for more efficient use of resources and to limit cross-border investigations to truly serious matters.

The Convention should not include "preventing" and "disrupting" cybercrime. It should also not form the basis for international cooperation on national security, cybersecurity initiatives such as intrusion detection and end-target hardening measures, or cyberwarfare.

Additionally, the Convention should not address the investigation or prosecution of civil or administrative matters. Nor should it form the basis

for attempts to achieve cybercrime objectives through techniques that fall outside the parameters of the criminal justice system.

For example, the use of states' offensive disruption measures (such as hacking end devices to interfere with the usage of the device or server, taking out botnets, and disrupting communications channels) or the imposition of preventive regulatory obligations onto service providers (such as obligations to secure their networks or services, investigate their customers or problematic traffic on their networks, or related obligations that are not about gathering evidence for criminal proceedings) should fall outside the scope of this Convention.

Finally, the Convention should include a Non-Discrimination Clause on the International Cooperation Provisions, and its language should be broader to also include "language, color, sexual orientation, and mental or physical disability."

On Question 3, Should the provisions on extradition and mutual legal assistance follow the models established by the United Nations Convention against Transnational Organized Crime or the United Nations Convention against Corruption, and, if so, to what extent?

In question 3, we believe it's important to note the significantly different context of communications service providers from other types of heavily-regulated private sector entities such as financial institutions and the importance of avoiding the imposition of any direct cooperation, offense discovery, or reporting obligations onto communications service providers. This is particularly so in light of the criminal justice focus that this Convention adopts (as opposed to cybersecurity threat mitigation).

EFF's Oral Intervention on Question 19

Delivered by George Wong

Written by Katitza Rodriguez

29 August to 9 September 2022, New York

Should the convention include a provision on transborder access to [data] [information]? It would allow for a State to access stored [computer data] [electronic information] without the authorization of the State party where such [data are] [information is] geographically located, if the [data are] [information is] publicly available, or if access to the [data] [information] is through a computer system located in its territory and that State obtains the consent of the person who has lawful authority to disclose the [data] [information] through that computer system. to their own nationals on a voluntary basis, as part of consular functions?

The Convention should explicitly emphasize existing MLAT arrangements as the primary means of achieving cross-border mutual assistance and should prioritize investment in states' existing MLAT processing mechanisms and central authorities. To the extent the Convention will supplement existing MLAT arrangements, the Convention should encourage states to afford each other mutual legal assistance to the fullest extent possible under relevant laws, treaties, agreements, and arrangements and enter into additional agreements based on MLAT principles. Requesting mutual assistance under such agreements should therefore continue to rely on a hosting state's central authority to process requests in reliance on its existing national law, rather than imposing obligations on states to adopt specific cross-border investigative powers.

The Convention should specifically refrain from encouraging, requiring, or authorizing states to bypass central authorities by sending requests directly

to service providers in hosting countries or through direct law enforcement interactions (spontaneous or otherwise).

6. How can consistency be ensured between international cooperation provisions and respect for human rights? A/AC.291/13 V.22-10829 3/6

7. How should the chapter on international cooperation determine the requirements for the protection of personal data for the purposes of the convention? Transmission of requests and materials

17. Should the convention include specific provisions on mutual legal assistance regarding provisional measures? If so, what specific provisions should be included? For example, should they include the expedited preservation of stored computer data and electronic information and expedited disclosure of preserved traffic data?

18. Should the convention include specific provisions on investigative powers? If so, what specific provisions should be included? For example, should they include access to stored computer data and electronic information, real-time collection of traffic data, and interception of content data?

On the Technical Assistance, Q. 24 & 25 & 28:
24. Which specific areas of technical assistance should be covered by the convention? 25. Which principles should be used to guide technical assistance and capacity-building efforts? Should these include drawing on best practices? 28. Which methods and means of providing technical assistance should be covered by the convention?

Technical Assistance Should Emphasize Training For Navigating The MLA Regime While Ensuring That Intrusive Techniques Do Not Threaten Human Rights.

To ensure a successful MLA regime, states should commit to providing other states with resources and training regarding the navigation of their respective national legal assistance frameworks. The Convention should require states to commit sufficient resources to provide this form of technical assistance.

We recommend caution regarding attempts to obligate assistance of a technical nature between states parties to the Convention, however. An increasingly intrusive array of surveillance tools are available to law enforcement, and these are frequently adopted and deployed without public discussion and approval at the national level. Many of the tools and techniques (e.g., device intrusion tools, zero-day exploits) can have far-ranging negative implications for the integrity of ICTs and can increase the possibility of cybercrime by introducing vulnerabilities into the ICT that criminals can exploit.

Once adopted, many of these tools and techniques have also been used for political repression and other problematic practices. The Convention should not become a vehicle for the broader dissemination and legitimization of these intrusive surveillance techniques.

Any framework for technical assistance should be limited to information exchange and training and not be construed to include shared operational deployment of intrusive surveillance tools or techniques nor to require the sharing of a specific method or capability. Any technical assistance should be accompanied by a rigorous human rights review to ensure technical capabilities are not used in a manner that contradicts the principle of legality, necessity, and proportionality or undermines the integrity of communications systems or is contrary to the states' constitutions.