24th August, 2022

Submission to the Third Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes

Katitza Rodríguez Pereda
Policy Director for Global Privacy
Electronic Frontier Foundation

EFF is an international civil society non-governmental organization registered under operative nine and has more than 39,000 members in 99 countries. EFF engages in strategic litigation in the United States and works in a range of international and national policy venues to promote and protect human rights and fundamental freedoms, foster innovation, and empower consumers.

EFF welcomes the opportunity to submit its comments to the Ad Hoc Committee for the third negotiating session, to be held from 29 August to 9 September, about provisions on international cooperation, conditions and safeguards, technical assistance, and preventive measures.

EFF would like to thank the Chairwoman, the Secretariat, and staffers for the critical work facilitating this process. While we are not convinced a global cybercrime treaty is necessary, we reiterate the need for a human-rights-by-design approach in the proposed UN Cybercrime treaty.

- The Scope of the Proposed International Cooperation Provisions Should be Restricted to Specific Serious Criminal Matters: The international cooperation components of the Convention should be limited in scope to investigations or prosecutions of specific crimes itemized in the Convention. It should be further limited in scope to include only 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 be narrow in scope and 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.

Also, 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, disrupting communications channels) or the imposition of preventative regulatory obligations onto service providers (obligations to secure their networks or services, obligations to 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.

- Include a Non-Discrimination Clause on the International Cooperation Provisions: The Convention should state that nothing in this Convention should be interpreted as imposing an obligation to extradite or to afford mutual legal assistance if the requested State Party has substantial grounds for believing that requests for extradition for offenses outlined in this Convention, or for mutual legal assistance concerning such offenses, have been made to prosecute or punish a person on account of that person's race, religion, nationality, ethnic origin or political opinion, or that compliance with the request would cause prejudice to that person's position for any of these reasons. We echo some Member States' suggestions to also include "language, color, sexual orientation, and mental or physical disability."

- Embed an MLAT-Based Approach: 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). We note, in particular, 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).

- International Cooperation Requires Detailed and Robust Freedom of Expression, Association, Privacy, Data Protection, Due Process, and Human Rights Conditions and Safeguards**:** Any timely international cooperation should go hand-in-hand with strong human rights protections and safeguards. Consistently enforcing international human rights in each state's application to its national investigative powers has proven challenging, as there are no adequate international law mechanisms for ensuring states meet their privacy obligations.

This is particularly so in cross-border contexts, where states do not always fully respect the privacy and other rights of foreign nationals. The Convention's human rights safeguards should therefore establish an adequate baseline of protection to ensure that states respond to legal assistance requests in a manner that respects human rights. The Convention should also not prevent states from adopting stronger human rights protections, nor should states be permitted to adopt weaker safeguards, including through case-by-case bilateral or multilateral agreements that rely on the Convention's cooperation mechanisms.

At a minimum, the Convention's safeguards should:

- explicitly prohibit any interference with the right to privacy, as well as any data processing that is not necessary, legitimate nor proportionate as defined in international human rights law;[1]
- be detailed and robust, and should ensure that privacy incursions are premised on independent authorization on the basis of a high degree of probability that the intrusion contemplated will yield evidence of a specific serious criminal offense;
- require states to reject any mutual legal assistance requests that do not respect the role of journalists, whistleblowers, political activists and dissidents, security researchers, LGBTQ communities, civil society organizations, or human rights defenders; and

[1] The Necessary and Proportionate principles draw on the rights to privacy, freedom of opinion and expression, and freedom of association as guaranteed in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), the European Charter on Fundamental Rights (EU Charter), and the Inter-American Convention on Human Rights (IACHR). While each of these rights is formulated in slightly different ways, the structure of each article is usually divided into two parts. The first paragraph sets out the core of the right, while the second paragraph sets out the circumstances in which that right may be restricted or limited. In summary, the right to privacy must be provided "by law"; It must not be "arbitrary"; It must pursue one of the legitimate aims exhaustively listed in that paragraph; and it must be "necessary" to achieve the aim in question—which has been held to include requirements of adequacy and proportionality. This "permissible limitations" test has been applied equally to the rights to privacy, freedom of expression, and freedom of association. Read more: Global Legal Analysis, Necessary and Proportionate Principles, https://necessaryandproportionate.org/global-legal-analysis/.

- establish clear data protection obligations that meet the highest standards among state parties with respect to personal information collected, used, disclosed, or retained in relation to the Convention.

Safeguards should also extend beyond formal requirements so that measures are in place to ensure privacy, data protection, due process, and human rights are fully realized in the implementation of the Convention. This should include regulatory oversight by independent quasi-judicial bodies empowered to audit, substantively review, and, where necessary, suspend cooperation arrangements between a host country and any other country that fails to provide adequate protection. It should also include the obligation to ensure states make available effective redress mechanisms at the national level and that these are also available to foreign nationals.

- International Cooperation Provisions May Encourage Cooperation Where Agencies are Investigating Similar Matters, but Joint Investigation Teams Should Not Form a Basis for Bypassing MLAT Mechanisms. The Convention's international cooperation provisions may encourage high-level information sharing in multi-jurisdiction investigations but should emphasize the need for a continual reliance on MLAT mechanisms as a basis for legal assistance.

- 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 the assistance of a technical nature 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.