Submission by Electronic Frontier Foundation and Privacy International to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose

Katitza Rodriguez
EFF Policy Director for Global Privacy

Tomaso Falchetta
Global Policy Lead, Privacy International

EFF is an international civil society non-governmental organization registered under operative 9, 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.

Privacy International is a non-governmental organization in consultative status with ECOSOC. PI researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilizes allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

Introduction

The Electronic Frontier Foundation (EFF) and Privacy International (PI) welcome the opportunity to submit its contribution for the second session of the Ad-Hoc Committee. While EFF and PI are not convinced a global cybercrime treaty is necessary, we believe it's important to reiterate the importance of having a human-rights-by-design approach in the proposed UN Cybercrime treaty. This priority was also addressed in a joint letter endorsed by 134 civil society organizations and experts in more than 56 countries and sent to the chairperson of the Ad-Hoc committee.[1]

This submission will address two topics. The first one relates to the section on Procedural & Investigative Criminal Measures and Law Enforcement, with a particular focus on cross-border investigative mechanisms. The second relates to the substantive criminal provision.

I. Procedural and Investigative Criminal Measures

1.1 The Proposed Convention Should Preserve the Same Human Rights Protections Traditionally Embedded in Mutual Legal Assistance Treaties (MLATs)

MLATs have historically provided the primary framework for government cooperation on cross-border criminal investigations. While specific details may vary across different MLATs, most share the same core human rights and procedural safeguards:

- A mechanism for requesting assistance to access data stored in a hosting country;
- A central authority that assesses and responds to assistance requests from foreign countries or refuses requests that are contrary to human rights;
- A legal basis in national law authorizing the central authority to obtain data on behalf of the requesting country; and
- The obligation for central authorities to rely on national search powers (and be bound by accompanying national privacy protections) when obtaining data in response to a request.

[1] Letter to the United Nations Ad Hoc Secretariat Asking to Include Human Rights Safeguards in Proposed Cybercrime Convention, https://www.eff.org/deeplinks/2022/02/letter-united-nations-include-human-rights-safeguards-proposed-cybercrime-treaty

In addition, prior to entering into an MLAT arrangement and implementing it into national law, states have typically assessed its compatibility with their respective legal systems to ensure core values and human rights standards will be respected before an arrangement is concluded.

Cross-border investigative cooperation should remain grounded in the MLAT regime, and any departures from that regime should retain these core elements.

1.2 Human Rights Should Not be Harmonized to the Lowest Common Denominator in Cross Border Investigations

The lawfulness and legitimacy of investigations depend on respect for criminal procedural safeguards, data protection, and human rights protections. If cross-border investigations are challenging, securing human rights in cross-border investigations is equally difficult. States should ensure that any interference with the right to privacy is based on publicly-accessible, precise, and non-discriminatory law, and is legitimate, necessary, and proportionate. Further, states should ensure that due process rights prevail, oversight mechanisms are applied, and immunity and privileges are respected. Finally, privacy rights interferences, such as gaining access to and sharing of data, should be authorized by a competent judicial authority that's impartial and independent. It is not enough to ensure that the investigative powers adopted by the treaty are capable of being employed in a manner that respects human rights—sufficient safeguards must already be in place to prevent the misuse of these powers.

A recent report of the UN Security Council's Counter-Terrorism Committee noted that, 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."[2]

As we state in our joint civil society letter, "there is a real risk that, in an attempt to entice all States to sign a proposed UN cybercrime convention, bad human rights practices will be accommodated, resulting in a race to the bottom." Bearing in mind the global nature of the proposed treaty, it will be crucial that human rights stay front and center during negotiations and that human rights protections are not eroded in the rush to expedite cross-border access.

[2] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), The state of international cooperation for lawful access to digital evidence: Research Perspectives, January 2022. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf

1.3 The Proposed Convention Should Explicitly Recognize that Access to Communications Data, Including Metadata and Subscriber Data, Can Be as Intrusive as Access to Content

Some negotiating states have suggested treating personal information safeguards in a hierarchical manner based on whether the data is categorized as "content data," "metadata," or "subscriber data." These categories don't reflect the privacy interests inherent in each data type, and should not form the basis for less privacy protection.

Non-content data includes, but is not limited to: contacts, the who, what, when, and where of our communications, map searches, visited websites, location information, as well as information, including technical identifiers, about every device connected to every network. When collected in aggregate about one or a number of individuals, it is no less—and can be even more—sensitive than the actual content of communications. This data makes it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, as well as identify the time of the communication and the place from which that communication originated. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.[3] Subscriber information can be used to identify individuals associated with online activity.

The understanding that access to metadata and subscriber data can be as intrusive as access to the content of communications has been long recognised by UN expert bodies.[4] As such, the distinction in privacy protections for content, metadata. or subscriber data is, in fact, no longer fit for purpose.

As a result, communications data, including metadata, should enjoy at least the same protections as content, and access to this data should be subject to the same conditions and protections as any other personal information.[5] To the extent that specific investigative powers are adopted to preserve or expedite access to metadata or subscriber data, narrow definitions of these data categories should be employed.

[3] Privacy International, Article19, and the Electronic Frontier Foundation Intervention in *Pietrzak v Poland*. http://hudoc.echr.coe.int/eng?i=001-199520
[4] UN High Commissioner for Human Rights Report Privacy in the Digital Age (2014), A/HRC/27/37, para. 19; 6.
[5] European Court of Human Rights, *Ekimdzhiev and others v. Bulgaria*, para. 394; Inter-American Court of Human Rights, *Escher and others v. Brazil*, para. 114; para. 115.

1.4 Any Effort To Enable Effective Police Investigations Should Go Hand-In-Hand With Respecting Critical Human Rights And Data Protection Safeguards

Any proposed law enforcement powers, and particularly any that interfere with privacy or personal information, should comply with the principle of legality, necessity, and proportionality,[6] and should be consistent with any applicable international law.[7] Moreover, it's imperative to apply robust protections when authorities are seeking cross-border access to personal data. As noted in numerous findings of UN human rights bodies, such interference should apply, regardless of the nationality or location of the individual concerned.[8] Nationality cannot be a criterion for lessening the safeguards applicable to procedural criminal measures, including the requirement of prior judicial authorisation.

To ensure the Treaty's investigative powers are not used in a manner that undermines human rights, the proposed treaty should also expressly note that its powers cannot be relied upon to impose obligations onto organizations to decrypt data or become capable of decrypting data. It should also expressly indicate that its powers cannot be used to impose data retention obligations of general purpose.

II. Substantive Criminal Provisions

2.1 The Scope of Criminal Conduct Covered Under the Definition of "Cybercrime" Should Be Narrow, Precise, and Specific

[6] UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/34/7 (23 March 2017); Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014); Report of the Special Rapporteur on the Right to Privacy, Visit to Argentina, UN Doc A/HRC/46/37/Add.5 (27 January 2021); Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN Doc A/75/590 (10 November 2020); Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015); Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014); Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013); Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018); Toonen v Australia, Comm No 488/1992, Human Rights Committee, UN Doc CCPR/C/50/D/488/1992 (31 March 1994); Inter-American Court of Human Rights, *Tristán Donoso v. Panamá*, para. 56;

[7] See also Privacy International,. Pi's Guide To International Law and Surveillance, https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

[8] See for example Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7, para. 24 (17 August 2015). For more references, please see Privacy International's Guide to International Law and Surveillance, December 2021, https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

EFF and PI have observed that, even as cybercrimes often threaten peoples' rights, risks to human rights have also arisen from vague and overbroad definitions of criminal offenses, and abusive applications of criminal law taken in the name of combating cybercrime. As OHCHR noted, we've seen "the common use at national levels of cybercrime laws and policies to restrict freedom of expression, target dissenting voices, justify Internet shutdowns, interfere with privacy and anonymity of communications, and limit the rights to freedom of association and peaceful assembly."[9]

The discussions at the prior sessions have shown that there is yet no shared global consensus on how to define cybercrime. From a human rights perspective, we respectfully suggest states emphasize narrowness, precision, and clarity on the scope of criminal conduct covered by the definition of cybercrime.

2.2 States Should Not Cast Too Wide a Net in Deciding What Crimes to Include in the Treaty

We would particularly wish to reiterate the need to focus on crimes that target information and communications technologies (ICTs). Core cybercrimes comprise offenses in which ICTs are the direct objects as well as instruments of the crimes; these crimes could not exist at all without the ICT systems. A useful reference for the types of crimes that are inherently ICT crimes can be found in Articles 2-6 of the Budapest Convention: illegal access to computing systems, illegal interception of communications, data interference, system interference, and misuse of devices. For example, spreading a computer virus in the wild; using a password logger to steal someone else's password and access their email or photos; breaking into the computer system of a bank to steal money; using malicious software to delete all the data of a former employer's systems.

2.3 Failure to Narrowly Define Cybercrime Can Result in Human Rights Abuses, Including the Targeting of Security Researchers' or Journalists' Legitimate Activities

When the definition of criminal conduct fails to require malicious intent or defines access "without authorization" too broadly, legitimate security research and journalism can be swept up by its definitions. "Without authorization" should be understood in a technical sense as bypassing an authorization system like a password requirement, as opposed to violations of a company's privacy policies.

2.4 Crimes Where ICTs Are Simply a Tool That is Sometimes Used in The Commission of an Offense Should be Excluded From the Treaty

These would include ordinary crimes already clearly and adequately prohibited under existing domestic legislation, and merely incidentally involve or benefit from ICT systems without

[9] OHCHR, Key-messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes, January 17, 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

targeting or harming those systems. For example, if a burglar used Google Maps in a crime, these information resources helped the criminal but the crime is still a physical-world crime and did not target ICT systems. The extortion of an individual where the demand is delivered by email. The act of extortion is already a crime and email may merely have been the means of delivering the threat.

2.5 If The Proposed Treaty Does Cover "Cyber-Enabled Crime," This Category Should Be Given a Narrow And Specific Definition, and Not Include Content Crimes.

Some states have proposed focusing the discussion through sub-categories such as "cyber-enabled crimes" but even such sub-categories have been used in rather inconsistent and varying ways by different states, and we would kindly suggest attempting to find agreement on the meaning of such categories and thereby defining them more explicitly.

2.6 We Would Particularly Caution Against the Inclusion of Any Content Crimes, Such as Extremism, Terrorism, Public Morals, Misinformation, or Hate Speech.

Content crimes are far outside of the core territory of cybercrime. They don't represent attacks or intrusions on ICT systems, and may well in many cases be authorized by the owners or operators of these systems. Further, content crimes are especially inconsistent and contradictory in matters of international cooperation. A lack of substantive consensus or equivalence between national laws exists in this area.

2.7 Regardless of What Crimes are Ultimately Included, They Must be Narrowly Defined with Clear Safeguards

Cybercrimes laws have been used against journalists, human rights defenders, politicians, lawyers, religious reformers, artists, whistleblowers and security researchers with devastating impact.