July 24, 2024

MEDIA BRIEFING
ORAL STATEMENT KATITZA RODRIGUEZ EFF POLICY DIRECTOR FOR GLOBAL PRIVACY

Thank you for being here today.

Cybersecurity is crucial for protecting our data and preventing cyberattacks. Yet, the UN's proposed cybercrime treaty undermines these efforts by threatening the vital work of security researchers who expose vulnerabilities to keep us safe. It could criminalize their essential work by broadly interpreting them as cybercrimes, without requiring malicious intent. We've seen researchers prosecuted under overbroad laws, and this treaty fails to learn from that history.

It also risks coercing tech employees, including those at NGOs, to compromise their systems' security. Article 28(4) allows states to order anyone with knowledge of a device or system to provide information needed for searches. This means bypassing normal channels and compelling engineers to break security systems, even without their employer's knowledge or against their own companies' policies. Worse, it could force people to reveal unfixed vulnerabilities to the government or disclose encryption keys, such as signing keys, for surveillance purposes. In countries with poor human rights records, this authority becomes a source of raw power. Failing to set clear limits on forcing technologists to reveal confidential information is a recipe for a cybersecurity disaster.

The UN's proposed cybercrime treaty threatens to formalize a global surveillance regime under the guise of combating cybercrime. It dangerously expands state surveillance powers across borders, compelling companies to act as agents of the state by monitoring and intercepting data in real time, often without users' knowledge or consent. These measures mandate total secrecy from service providers, preventing users from ever knowing if their data was misused. This perpetual secrecy eliminates transparency and accountability, making it impossible for individuals to challenge or seek redress for abuses. As a result, the treaty becomes a powerful tool for countries with poor human rights records, enabling them to pressure companies into assisting with surveillance practices that undermine the rule of law and human rights. This, in turn, puts users' personal data at risk, allowing these governments to extend their repressive practices beyond their borders, targeting political opponents, dissidents, and activists who seek refuge in other countries.

Even worse, the treaty's broad scope would compel companies to assist in surveillance to investigate acts of expression that certain countries with poor human rights records deem criminal. Chapter 5, Article 40, requires "the widest measure of mutual legal assistance" for serious offenses under domestic law. Previously, many countries didn't establish MLATs due to valid human rights concerns. Now, the proposed treaty obligates State Parties to provide

mutual legal assistance for those without an MLAT, often with insufficient human rights safeguards, ignoring these valid concerns. Article 40, paragraph 22, sets a high bar for refusal, requiring “substantial grounds for believing” the request is improper, making it difficult to deny assistance even when human rights are at risk. Worse, using these avenues is discretionary, meaning states can comply with these requests even if they have valid human rights concerns. Instead of forbidding states from complying with requests they believe involve persecution, the text simply says they have no "obligation" to assist in these cases.

As the Convention aims for worldwide adoption, it is likely to be signed and implemented by countries with poor human rights records. Yet the text frequently makes human rights safeguards optional and discretionary, allowing these countries to define "appropriate" protections under their national laws, which can be as weak as their ruling elites desire. Moreover, when these countries conduct surveillance on behalf of others, their ability to refuse improper requests is disturbingly limited.

The Convention is silent on many essential rules for electronic surveillance and searches. It does not require law enforcement to respect privileges like attorney-client or physician-patient privilege, nor does it protect suspects from self-incrimination. While we hope that domestic laws will include these protections, the Convention fails to mandate them. If adopted, the Convention will be enforced by states with varying legal standards, risking a drop to the lowest human rights protections.

While some states with poor human rights records may already cooperate to spy on dissenting groups, this treaty would cement such oppression with the legitimacy and support of the United Nations, providing a dangerous legal basis for these actions. It also seeks to turn companies into agents of control, compelling them to assist in surveillance practices that undermine the rule of law. Such practice must be outside the scope of the treaty, not merely suggesting respecting human rights within the broad scope of the treaty, which we support but insufficient.

Countries that believe in the rule of law must do everything they can to avoid providing a legal basis for spying activities that should be condemned globally.

Some states may argue that this Convention doesn't change existing practices. We disagree. By not making human rights safeguards explicit, by not narrowing the treaty’s scope, and by telling its signatories to spy widely, routinely, and uncritically on each other’s behalf, the draft treaty effectively grants countries with poor human rights records a blank check for abuse.

Thank you,

Frequently Asked Questions

Question: How have cybersecurity researchers been prosecuted or threatened for their work?
Read: From Canada to Argentina, Security Researchers Have Rights

Question: What is the lesson that the treaty failed to learn from prior experiences involving cybersecurity researchers?

Answer: Now, just as some governments have finally recognized the importance of protecting security researchers' work, many of the UN convention's criminalization provisions threaten to spread antiquated and ambiguous language around the world with no meaningful protections for researchers or journalists. This oversight is alarming. If these and other issues are not addressed, the convention poses a global threat to cybersecurity and press freedom, and UN Member States must reject it.

- Many of the criminalization provisions threaten to spread outdated and ambiguous language, harming both researchers and journalists.
- The draft treaty fails to distinguish between malicious hacking and good-faith cybersecurity research, putting researchers at risk globally.
- The requirement for malicious intent must be mandatory to protect those who seek to improve security, not criminalize them.
- Without explicit exemptions for security research, the protections researchers have fought for at national levels are not guaranteed internationally, across borders.
- The lack of clear distinctions between malicious unauthorized access and security research creates legal uncertainty and jeopardizes crucial cybersecurity work.
- We need definitions that focus on bypassing effective security measures with harmful intent, not good-faith efforts to identify vulnerabilities.

Question: Why don't you trust states with poor human rights records in regulating the work of security researchers?

States with poor human rights records may misuse cybersecurity regulations to control and exploit security research, compromising global security and leaving users vulnerable. This approach prioritizes state power over genuine cybersecurity improvements.

States with poor human rights records often lack transparency and accountability. These states may use cybersecurity laws to suppress independent security research, rather than genuinely protecting security. Restrictions on security researchers can prevent them from disclosing vulnerabilities to the public or responsible vendors. This can leave systems vulnerable to exploitation, as the information about the vulnerabilities is kept secret by the state. For example, China's cybersecurity law requires researchers to report vulnerabilities to the government rather than the affected parties. This means vulnerabilities are not promptly fixed, increasing the risk for everyone.

By controlling security research, states can enhance their own hacking capabilities. This co-opts the research community to serve state interests, rather than improving overall cybersecurity. Such policies leave end-users, both domestically and internationally, more vulnerable to hacking. The state may withhold critical information about vulnerabilities, putting everyone at greater risk.

Question: What is the lesson that the treaty failed to learn from prior experiences involving cybersecurity researchers?

Answer: The draft treaty failed to learn a critical lesson from prior experiences involving cybersecurity researchers: the importance of protecting their work. Despite some governments finally recognizing the value of cybersecurity researchers, many of the UN convention's criminalization provisions threaten to spread outdated and ambiguous language globally, offering no meaningful protections for researchers or journalists. This oversight is alarming and, if unaddressed, poses a global threat to cybersecurity and press freedom, which UN Member States must reject.

- The draft treaty failed to adequately distinguish between malicious hacking and good-faith cybersecurity research, putting researchers at risk worldwide. The lack of clear distinctions between malicious unauthorized access and legitimate security research creates legal uncertainty and jeopardizes crucial cybersecurity work. This is why it is imperative that the draft treaty mandates malicious intent—defined as an intent to cause damage, defraud, or harm—to ensure that those who seek to improve security are protected and not criminalized.
- The draft treaty must also define "without right" as bypassing an effective security measure with harmful intent, not good-faith efforts to identify vulnerabilities. This means that only actions that involve bypassing effective security measures with the intent to cause damage, defraud, or harm would be considered illegal. By doing so, the treaty would clearly differentiate between malicious unauthorized access and legitimate security research, providing a safer environment for researchers to operate and contribute to global cybersecurity.
- Last but not least, the draft treaty should include explicit exemptions for security research. Without these, the protections that researchers have fought for at national levels are not guaranteed internationally, across borders.

Question: Doesn't Article 11, paragraph 2, protect security researchers by not imposing criminal liability if the use or possession of the tool is "not for the purpose of committing an offence established" under the treaty?

Answer: Article 11, paragraph 2 of the draft treaty does provide some protection for security researchers by stating that criminal liability does not apply if the possession or use of a tool is not for the purpose of committing an offense established under the treaty. Specifically, it mentions "the authorized testing or protection of an information and communications technology system" as examples of protected activities. However, there are significant concerns regarding the effectiveness of this protection.

The offenses outlined in Articles 7 to 10 of the draft treaty are defined in broad terms, and the consistent use of the phrase "without right" creates ambiguity about what constitutes authorized versus unauthorized activities. This lack of clarity can lead to varied interpretations

by different states, potentially criminalizing activities that are not explicitly authorized but are necessary for security research.

For non-experts, this means that while Article 11, paragraph 2 is supposed to protect researchers, the vague language in the treaty can still result in security researchers being accused of illegal activity. Security researchers often test systems to find and fix vulnerabilities without explicit permission, which is crucial for maintaining cybersecurity. However, the treaty's requirement for "authorized testing" implies that researchers need prior explicit permission, which is not always feasible or practical in real-world scenarios. This could lead to researchers being unfairly targeted despite their intention to improve security. Thus, the protection offered by Article 11, paragraph 2 is undermined by the broader, unclear definitions in the treaty, potentially subjecting security researchers to criminal liability.

Question: Aren't some of these criminal provisions already part of the existing Budapest Convention? Do you have examples of how they were abused or didn't work as expected when implemented pursuant to the existing convention?

- Yes, some provisions are indeed part of the existing Budapest Convention. However, the experience with the Budapest Convention has shown that these provisions can be problematic when applied without clear safeguards. For example, the lack of explicit mandatory protections for cybersecurity researchers has led to cases where security researchers were prosecuted despite their intentions to improve security. Read the answer above.
- From these experience, we've learned that certain safeguards must be mandatory, not optional, to protect cybersecurity researchers:
    - Define "without right" as bypassing an effective security measure with harmful intent, not good-faith efforts to identify vulnerabilities.
    - Require malicious intent—defined as an intent to cause damage, defraud, or harm—to ensure that those who seek to improve security are protected and not criminalized.

Question: Some states have said that this treaty doesn't actually change substantive rules about law enforcement powers or cooperation, just clarifies them or makes them more explicit. How do you respond to this?

Answer: While the proposed treaty might appear to clarify existing rules, in reality, it significantly expands law enforcement powers and cooperation mechanisms without adequate safeguards. The draft treaty introduces new requirements for real-time surveillance and data interception that go far beyond current practices, compelling companies to assist in ways they previously were not obligated to. This expansion of powers includes mandatory cooperation with foreign law enforcement agencies, even in countries with poor human rights records, which raises serious concerns about abuse and misuse. Even if the treaty includes human rights safeguards in its text, countries with poor human rights records can exploit vague definitions to justify repressive actions, applying these powers arbitrarily and oppressively. Safeguards alone

are not enough. We need to ensure the independence of the judiciary, robust accountability mechanisms, and effective oversight to prevent misuse and protect human rights.

Question: For example, don't states already have some amount of power to require wiretaps, to perform searches of digital devices, or even to compel companies to provide technical assistance with surveillance?

Answer: Yes, states do have existing powers to require wiretaps, conduct searches of digital devices, and compel companies to provide technical assistance with surveillance under their domestic law. However, this treaty would dangerously expand these powers by providing a legal basis for surveillance in investigations of any crimes defined by domestic laws, which often include expression crimes. Furthermore, it would force companies to assist in surveillance for any crime at the discretion of national authorities.

In countries with poor human rights records, such obligations could force companies to comply with requests that infringe on privacy and freedom of expression, violating the principles of the rule of law and companies' commitments under the UN Guiding Principles on Business and Human Rights. These principles oblige companies to respect human rights, avoid infringing on the rights of others, and address adverse human rights impacts with which they are involved. In certain countries, this could lead to companies being complicit in human rights abuses by complying with oppressive surveillance requests.

It is essential for international agreements to uphold the highest standards of human rights, ensuring that any surveillance measures are conducted with transparency, accountability, and respect for the rule of law. This approach will help protect both companies and users from being complicit in or victims of state overreach and human rights violations.

Question: What rules or provisions would you specifically want to be added to the safeguard sections? What would that look like? How would the safeguards actually be written to protect the other principles on surveillance that you talk about, or the right against self-incrimination?

Answer: To ensure robust safeguards in the treaty, we recommend adding specific provisions that protect privileged communications, prevent self-incrimination, and uphold the fairness of criminal proceedings, and protect personal data.

For example, many countries' have various kinds of information that is protected by a legal "privilege" against surveillance: attorney-client privilege, the spousal privilege, the priest-penitent privilege, doctor-patient privileges, and many kinds of protections for confidential business information and trade secrets. Many countries also give additional protections for journalists and their sources. These categories, and more, provide varying degrees of extra requirements before law enforcement may access them using production orders or search-and-seizure powers, as well as various protections after the fact, such as

preventing their use in prosecutions or civil actions.

Similarly, the convention lacks clear safeguards to prevent authorities from compelling individuals to provide evidence against themselves. These omissions raise significant red flags about the potential for abuse and the erosion of fundamental rights when a treaty text involves so many countries with a high disparity of human rights protections.

The lack of specific protections for criminal defense is especially troubling. In many legal systems, defense teams have certain protections to ensure they can effectively represent their clients, including access to exculpatory evidence and the protection of defense strategies from surveillance. However, the draft convention does not explicitly protect these rights, which both **misses the chance to require all countries** to provide these minimal protections and potentially further undermines the fairness of criminal proceedings and the ability of suspects to mount an effective defense in countries that either don't provide those protections or where they are not solid and clear.

Question: What was this about the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)? How does this treaty relate to the CLOUD Act and the controversies over its powers and which countries can invoke it? How would this treaty change the behavior of the U.S. and of the major U.S. tech companies, which hold so much of the world's data?

Answer: The CLOUD Act has been controversial due to its lack of stringent safeguards and several key issues that have not been addressed. The executive agreement language has been criticized for:

- Including a weak standard for review that does not meet the protections of the warrant requirement under the 4th Amendment.
- Failing to require foreign law enforcement to seek individualized and prior judicial review.
- Granting real-time access and interception to foreign law enforcement without requiring the heightened warrant standards that U.S. police must adhere to under the Wiretap Act.
- Failing to place adequate limits on the category and severity of crimes for this type of agreement.
- Failing to require notice at any level—to the person targeted, to the country where the person resides, and to the country where the data is stored.

The proposed UN Cybercrime Convention introduces even more significant concerns. While the CLOUD Act involves bilateral agreements and some level of negotiation, the Cybercrime Convention would allow any signatory state to request data from any other signatory state on an equal basis. Although this approach sounds fair in principle, the real problem emerges when considering human rights safeguards, the varying human rights records of different countries, and the broad scope of crimes as defined by national laws.

Countries with poor human rights records could exploit the treaty to access data, leading to widespread abuses. Even governments with strong protections for free expression and privacy at home have proven unreliable defenders of rights when it comes to international cooperation, often compromising these standards in the name of countering terrorism or other serious crimes. This treaty, by allowing data requests for any crime as defined by national laws, risks lowering the bar for privacy protections globally.

The UN has the opportunity to draft a treaty that includes robust safeguards, is narrow in scope, and ensures that international cooperation on cybercrime does not come at the expense of human rights. It is crucial to establish clear and enforceable protections to prevent potential abuses and uphold the principles of human rights and the rule of law. What is really disappointing is that when it comes to police trying to access data across borders, the discussion is focused on lowering safeguards rather than making them stronger. This trend represents a dangerous race to the bottom in privacy protections, and the UN must take a stand to reverse it and set a higher standard for global privacy rights.