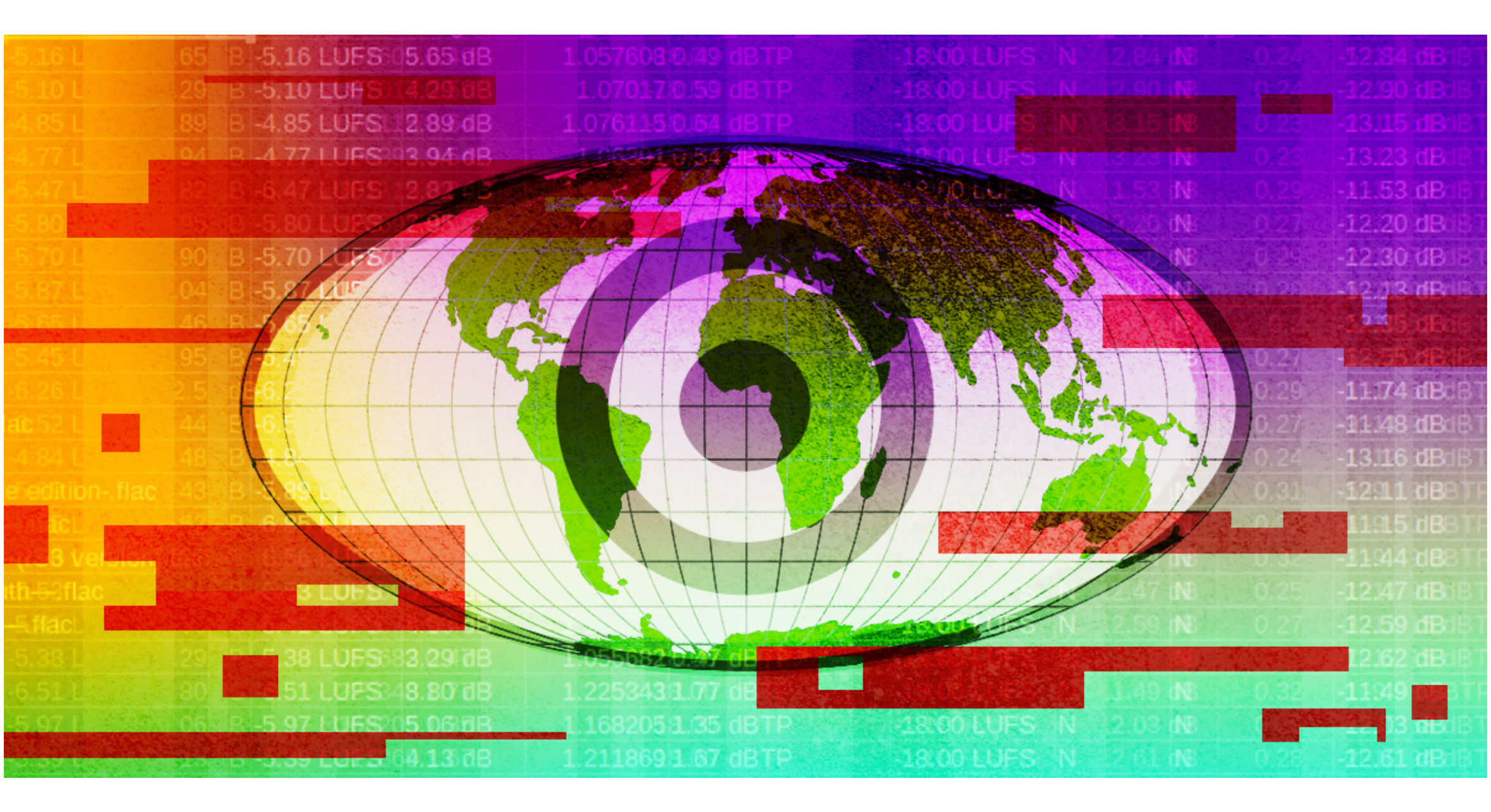
The UN Cybercrime Draft Convention is a Blank Check for Surveillance Abuses

BY KATITZA RODRIGUEZ | JUNE 14, 2024



This is the second post in a series highlighting the problems and flaws in the proposed UN Cybercrime Convention. Check out our detailed analysis on the criminalization of security research activities under the proposed convention.

The United Nations Ad Hoc Committee is just weeks away from finalizing a too-broad Cybercrime Draft Convention. This draft would normalize unchecked domestic surveillance and rampant government overreach, allowing serious human rights abuses around the world.

The latest draft of the convention—originally spearheaded by Russia but since then the subject of two and a half years of negotiations—still authorizes broad surveillance powers without robust safeguards and fails to spell out data protection principles essential to prevent government abuse of power.

As the August 9 finalization date approaches, Member States have a last chance to address the convention's lack of safeguards: prior judicial authorization, transparency, user notification, independent oversight, and data protection principles such as transparency, minimization, notification to users, and purpose limitation. If left as is, it can and will be wielded as a tool for systemic rights violations.

Countries committed to human rights and the rule of law must unite to demand stronger data protection and human rights safeguards or reject the treaty altogether. These domestic surveillance powers are critical as they underpin international surveillance cooperation.

EFF's Advocacy for Human Rights Safeguards

EFF has consistently advocated for human rights safeguards to be a baseline for both the criminal procedural measures and international cooperation chapters. The collection and use of digital evidence can implicate human rights, including privacy, free expression, fair trial, and data protection. Strong safeguards are essential to prevent government abuse.

Regrettably, many states already fall short in these regards. In some cases, surveillance laws have been used to justify overly broad practices that disproportionately target individuals or groups based on their political views—particularly ethnic and religious groups. This leads to the suppression of free expression and association, the silencing of dissenting voices, and discriminatory practices. Examples of these abuses include covert surveillance of internet activity without a warrant, using technology to track individuals in public, and monitoring private communications without legal authorization, oversight, or safeguards.

The Special Rapporteur on the rights to freedom of peaceful assembly and of association has already sounded the alarm about the dangers of current surveillance laws, urging states to revise and amend these laws to comply with international human rights norms and standards governing the rights to privacy, free expression, peaceful assembly, and freedom of association. The UN Cybercrime Convention must be radically amended to avoid entrenching and expanding these existing abuses globally. If not amended, it must be rejected outright.

How the Convention Fails to Protect Human Rights in Domestic Surveillance

The idea that checks and balances are essential to avoid abuse of power is a basic "Government 101" concept. Yet throughout the negotiation process, Russia and its allies have sought to chip away at the already-weakened human rights safeguards and conditions outlined in Article 24 of the proposed Convention.

Article 24 as currently drafted requires that every country that agrees to this convention must ensure that when it creates, uses, or applies the surveillance powers and procedures described in the domestic procedural measures, it does so under its own laws. These laws must protect human rights and comply with international human rights law. The principle of proportionality must be respected, meaning any surveillance measures should be appropriate and not excessive in relation to the legitimate aim pursued.

Why Article 24 Falls Short?

1. The Critical Missing Principles

While incorporation of the principle of proportionality in Article 24(1) is commendable, the article still fails to explicitly mention the principles of legality, necessity, and non-discrimination, which hold equivalent status to proportionality in human rights law relative to surveillance activities. A primer:

- The principle of legality requires that restrictions on human rights including the right to privacy be authorized by laws that are clear, publicized, precise, and predictable, ensuring individuals understand what conduct might lead to restrictions on their human rights.
- The principles of necessity and proportionality ensure that any interference with human rights is demonstrably necessary to achieving a legitimate aim and only include measures that are proportionate to that aim.
- The principle of non-discrimination requires that laws, policies and human rights obligations be applied equally and fairly to all individuals, without any form of discrimination based on race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status, including the application of surveillance measures.

Without including all these principles, the safeguards are incomplete and inadequate, increasing the risk of misuse and abuse of surveillance powers.

2. Inadequate Specific Safeguards

Article 24(2) requires countries to include, where "appropriate," specific safeguards like:

- judicial or independent review, meaning surveillance actions must be reviewed or authorized by a judge or an independent regulator.
- the right to an effective remedy, meaning people must have ways to challenge or seek remedy if their rights are violated.
- justification and limits, meaning there must be clear reasons for using surveillance and limits on how much surveillance can be done and for how long.

Article 24 (2) introduces three problems:

2.1 The Pitfalls of Making Safeguards Dependent on Domestic Law

Although these safeguards are mentioned, making them contingent on domestic law can vastly weaken their effectiveness, as national laws vary significantly and many of them won't provide adequate protections.

2.2 The Risk of Ambiguous Terms Allowing Cherry-Picked Safeguards

The use of vague terms like "as appropriate" in describing how safeguards will apply to individual procedural powers allows for varying interpretations, potentially leading to weaker protections for certain types of data in practice. For example, many states provide minimal or no safeguards for accessing subscriber data or traffic data despite the intrusiveness of resulting surveillance practices. These powers have been used to identify anonymous online activity, to locate and track people, and to map people's contacts. By granting states broad discretion to decide which safeguards to apply to different surveillance powers, the convention fails to ensure the text will be implemented in accordance with human rights law. Without clear mandatory requirements, there is a real risk that essential protections will be inadequately applied or omitted altogether for certain specific powers, leaving vulnerable populations exposed to severe rights violations. Essentially, a country could just decide that some human rights safeguards are superfluous for a particular kind or method of surveillance, and dispense with them, opening the door for serious human rights abuses.

2.3 Critical Safeguards Missing from Article 24(2)

The need for prior judicial authorization, for transparency, and for user notification is critical to any effective and proportionate surveillance power, but not included in Article 24(2).

Prior judicial authorization means that before any surveillance action is taken, it must be approved by a judge. This ensures an independent assessment of the necessity and proportionality of the surveillance measure before it is implemented. Although Article 24 mentions judicial or other independent review, it lacks a requirement for prior judicial authorization. This is a significant omission that increases the risk of abuse and infringement on individuals' rights. Judicial authorization acts as a critical check on the powers of law enforcement and intelligence agencies.

Transparency involves making the existence and extent of surveillance measures known to the public; people must be fully informed of the laws and practices governing surveillance so that they can hold authorities accountable. Article 24 lacks explicit provisions for transparency, so surveillance measures could be conducted in secrecy, undermining public trust and preventing meaningful oversight. Transparency is essential for ensuring that surveillance powers are not misused and that individuals are aware of how their data might be collected and used.

User notification means that individuals who are subjected to surveillance are informed about it, either at the time of the surveillance or afterward when it no longer jeopardizes the investigation. The absence of a user notification requirement in Article 24(2) deprives people of the opportunity to challenge the legality of the surveillance or seek remedies for any violations of their rights. User notification is a key component of protecting individuals' rights to privacy and due process. It may be delayed, with appropriate justification, but it must still eventually occur and the convention must recognize this.

Independent oversight involves monitoring by an independent body to ensure that surveillance measures comply with the law and respect human rights. This body can investigate abuses, provide accountability, and recommend corrective actions. While Article 24 mentions judicial or independent review, it does not establish a clear mechanism for ongoing independent oversight. Effective oversight requires a dedicated, impartial body with the authority to review surveillance activities continuously, investigate complaints, and enforce compliance. The lack of a robust oversight mechanism weakens the framework for protecting human rights and allows potential abuses to go unchecked.

Conclusion

While it's somewhat reassuring that Article 24 acknowledges the binding nature of human rights law and its application to surveillance powers, it is utterly unacceptable how vague the article remains about what that actually means in practice. The "as appropriate" clause is a dangerous loophole, letting states implement intrusive powers with minimal limitations and no prior judicial authorization, only to then disingenuously claim this was "appropriate." This is a blatant invitation for abuse. There's nothing "appropriate" about this, and the convention must be unequivocally clear about that.

This draft in its current form is an egregious betrayal of human rights and an open door to unchecked surveillance and systemic abuses. Unless these issues are rectified, Member States must recognize the severe flaws and reject this dangerous convention outright. The risks are too great, the protections too weak, and the potential for abuse too high. It's long past time to stand firm and demand nothing less than a convention that genuinely safeguards human rights.

Check out our detailed analysis on the criminalization of security research activities under the UN Cybercrime Convention. Stay tuned for our next post, where we'll explore other critical areas affected by the convention, including its scope and human rights safeguards.

RELATED ISSUES:
UNITED NATIONS CYBERCRIME TREATY
NECESSARY AND PROPORTIONATE

RELATED UPDATES

DEEPLINKS BLOG BY KATITZA RODRIGUEZ | JUNE 14, 2024

If Not Amended, States Must Reject the Flawed Draft UN Cybercrime Convention Criminalizing Security Research and Certain Journalism Activities

This is the first post in a series highlighting the problems and flaws in the proposed UN Cybercrime Convention. Check out The UN Cybercrime Draft Convention is a Blank Check for Surveillance Abuses. The latest and nearly final version of the proposed UN Cybercrime Convention—dated May 23, 2024...

DEEPLINKS BLOG BY KAREN GULLO | MAY 23, 2024

NETMundial+10 Multistakeholder Statement Pushes for Greater Inclusiveness in Internet Governance Processes

A new statement about strengthening internet governance processes emerged from the NETMundial +10 meeting in Brazil last month, strongly reaffirming the value of and need for a multistakeholder approach involving full and balanced participation of all parties affected by the internet—from users, governments, and private companies to civil society, technologists,...

DEEPLINKS BLOG BY KAREN GULLO | FEBRUARY 7, 2024

Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty

Statement submitted to the UN Ad Hoc Committee Secretariat by the Electronic Frontier Foundation, accredited under operative paragraph No. 9 of UN General Assembly Resolution 75/282, on behalf of 124 signatories. We, the undersigned, representing a broad spectrum of the global security research community, write to express our serious concerns...

DEEPLINKS BLOG BY KAREN GULLO | FEBRUARY 7, 2024

Draft UN Cybercrime Treaty Could Make Security Research a Crime, Leading 124 Experts to Call on UN Delegates to Fix Flawed Provisions that Weaken Everyone's Security

Security researchers' work discovering and reporting vulnerabilities in software, firmware, networks, and devices protects people, businesses and governments around the world from malware, theft of critical data, and other cyberattacks. The internet and the digital ecosystem are safer because of their work.The UN Cybercrime Treaty,...

DEEPLINKS BLOG BY KAREN GULLO | JANUARY 29, 2024

In Final Talks on Proposed UN Cybercrime Treaty, EFF Calls on Delegates to Incorporate Protections Against Spying and Restrict Overcriminalization or Reject Convention

Update: Delegates at the concluding negotiating session failed to reach consensus on human rights protections, government surveillance, and other key issues. The session was suspended Feb. 8 without a final draft text. Delegates will resume talks at a later day with a view to concluding their work and providing a...

DEEPLINKS BLOG BY GEORGE WONG | JANUARY 23, 2024

EFF and More Than 100+ NGOS Set Non-Negotiable Redlines Ahead of UN Cybercrime Treaty Negotiations

EFF has joined forces with 110 NGOs today in a joint statement delivered to the United Nations Ad Hoc Committee, clearly outlining civil society non-negotiable redlines for the proposed UN Cybercrime Treaty, and asserting that states should reject the proposed treaty if these essential changes are not...

DEEPLINKS BLOG BY JILLIAN C. YORK | JANUARY 10, 2024

UAE Confirms Trial Against 84 Detainees; Ahmed Mansoor Suspected Among Them

The UAE confirmed this week that it has placed 84 detainees on trial, on charges of "establishing another secret organization for the purpose of committing acts of violence and terrorism on state territory." Suspected to be among those facing trial is award-winning human rights defender Ahmed Mansoor,...

DEEPLINKS BLOG BY KATITZA RODRIGUEZ | DECEMBER 1, 2023

Latest Draft of UN Cybercrime Treaty Is A Big Step Backward

A new draft of the controversial United Nations Cybercrime Treaty has only heightened concerns that the treaty will criminalize expression and dissent, create extensive surveillance powers, and facilitate cross-border repression. The proposed treaty, originally aimed at combating cybercrime, has morphed into an...

DEEPLINKS BLOG BY ELECTRONIC FRONTIER FOUNDATION | SEPTEMBER 29, 2023

The Growing Threat of Cybercrime Law Abuse: LGBTQ+ Rights in MENA and the UN Cybercrime Draft Convention

This is Part II of a series examining the proposed UN Cybercrime Treaty in the context of LGBTQ+ communities. Part I looks at the draft Convention's potential implications for LGBTQ+ rights. Part II provides a closer look at how cybercrime laws might specifically impact the LGBTQ+ community and activists...

DEEPLINKS BLOG BY KAREN GULLO | SEPTEMBER 13, 2023

UN Cybercrime Treaty Talks End Without Consensus on Scope And Deep Divides About Surveillance Powers

As the latest negotiating session on the proposed UN Cybercrime Treaty wrapped up in New York earlier this month, one thing was clear: with time running out to finalize the text, little progress and consensus was reached on crucial points, such as the treaty's overall scope of...