Still Flawed and Lacking Safeguards, UN Cybercrime Treaty Goes Before the UN General Assembly, then States for Adoption

Karen Gullo ⋮ 6-8 minutes ⋮ 12/17/2024

Update (12/21/24): A vote on the UN Cybercrime Treaty by the UN General Assembly was postponed to a later date to allow time for a review of its budget implications. The new date for the vote was not set.

Most UN Member States, including the U.S., are expected to support adoption of the flawed UN Cybercrime Treaty when it's scheduled to go before the UN General Assembly this week for a vote, despite warnings that it poses dangerous risks to human rights.

EFF and its civil society partners–along with cybersecurity and internet companies, press organizations, the International Chamber of Congress, the United Nations High Commissioner for Human Rights, and others–for years have raised red flags that the treaty authorizes open-ended evidence gathering powers for crimes with little nexus to core cybercrimes, and has minimal safeguards and limitations.

The final draft, unanimously approved in August by over 100 countries that had participated in negotiations, will permit intrusive surveillance practices in the name of engendering cross-border cooperation.

The treaty that will go before the UN General Assembly contains many troubling provisions and omissions that don't comport with international human rights standards and leave the implementation of human rights safeguards to the discretion of Member States. Many of these Member States have poor track records on human rights and national laws that don't protect privacy while criminalizing free speech and gender expression.

Thanks to the work of a coalition of civil society groups that included EFF, the U.S. now seems to recognize this potential danger. In a statement by the U.S. Deputy Representative to the Economic and Social Council, the U.S. said it "shares the legitimate concerns" of industry and civil society, which warned that some states could leverage their human rights-challenged national legal frameworks to enable transnational repression.

We expressed grave concerns that the treaty facilitates requests for user data that will enable cross-border spying and the targeting and harassment of those, for example, who expose and work against government corruption and abuse. Our full analysis of the treaty can be found here.

Nonetheless, the U.S. said it will support the convention when it comes up for this vote, noting among other things that its terms don't permit parties from using it to violate or suppress human rights.

While that's true as far as it goes, and is important to include in principle, some Member States' laws empowered by the treaty already fail to meet human rights standards. And the treaty fails to adopt specific safeguards to truly protect human rights.

The safeguards contained in the convention, such as the need for judicial review in the chapter on procedural measures in criminal investigations, are undermined by being potentially discretionary and contingent on state's domestic laws. In many countries, these domestic laws don't require judicial authorization based on reasonable suspicion for surveillance and or real-time collection of traffic.

For example, our partner Access Now points out that in Algeria, Lebanon, Palestine, Tunisia, and Egypt, cybercrime laws require telecommunications service providers to preemptively and systematically collect large amounts of user data without judicial authorization.

Meanwhile, Jordan's cybercrime law has been used against LGBTQ+ people, journalists, human rights defenders, and those criticizing the government.

The U.S. says it is committed to combating human rights abuses by governments that misuse national cybercrime statues and tools to target journalists and activists. Implementing the treaty, it says, must be paired with robust domestic safeguards and oversight.

It's hard to imagine that governments will voluntarily revise cybercrime laws as they ratify and implement the

treaty; what's more realistic is that the treaty normalizes such frameworks.

Advocating for improvements during the two years-long negotiations was a tough slog. And while the final version is highly problematic, civil society achieved some wins. An early negotiating document named 34 purported cybercrime offenses to be included, many of which would criminalize forms of speech. Civil society warned of the dangers of including speech-related offenses; the list was dropped in later drafts.

Civil society advocacy also helped secure specific language in the general provision article on human rights specifying that protection of fundamental rights includes freedom of expression, opinion, religion, conscience, and peaceful assembly. Left off the list, though, was gender expression.

The U.S., meanwhile, has called on all states "to take necessary steps within their domestic legal systems to ensure the Convention will not be applied in a manner inconsistent with human rights obligations, including those relating to speech, political dissent, and sexual identity."

Furthermore, the U.S. government pledges to demand accountability – without saying how it will do so – if states seek to misuse the treaty to suppress human rights. "We will demand accountability for States who try to abuse this Convention to target private companies' employees, good-faith cybersecurity researchers, journalists, dissidents, and others." Yet the treaty contains no oversight provisions.

The U.S. said it is unlikely to sign or ratify the treaty "unless and until we see implementation of meaningful human rights and other legal protections by the convention's signatories."

We'll hold the government to its word on this and on its vows to seek accountability. But ultimately, the destiny of the U.S declarations and the treaty's impact in the U.S are more than uncertain under a second Trump administration, as ratification would require both the Senate's consent and the President's formal ratification.

Trump withdrew from climate, trade, and arms agreements in his first term, so signing the UN Cybercrime Treaty may not be in the cards – a positive outcome, though probably not motivated by concerns for human rights.

Meanwhile, we urge states to vote against adoption this week and not ratify the treaty at home. The document puts global human rights at risk. In a rush to to win consensus, negotiators gave Member States lots of leeway to avoid human rights safeguards in their "criminal" investigations, and now millions of people around the world might pay a high price.

Join EFF Lists