

United States Senate

WASHINGTON, DC 20510

October 29, 2024

The Honorable Antony Blinken
Secretary of State
U.S. Department of State
2201 C Street NW
Washington, D.C. 20520

The Honorable Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

The Honorable Gina Raimondo
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, D.C. 20230

Jake Sullivan
Assistant to the President for
National Security Affairs
The White House
Washington, D.C. 20500

Dear Secretary Blinken, Attorney General Garland, Secretary Raimondo and Mr. Sullivan:

We write to express serious concern about the recently finalized United Nations (U.N.) Convention Against Cybercrime (the Convention), which will soon receive a vote in the U.N. General Assembly (UNGA). We fear the Convention will legitimize efforts by authoritarian countries like Russia and China to censor and surveil internet users, furthering repression and human rights abuses around the world. While the Executive Branch's efforts to steer this treaty in a less-harmful direction are commendable, more must be done to keep the Convention from being used to justify such actions.

Since 2001, transnational efforts to fight cybercrime have been governed largely by the Budapest Convention. Neither Russia nor China is a signatory to the Budapest Convention, and Russia has long sought to supplant the Budapest Convention with a new framework that the Russian regime could more easily influence. In 2017, Russia proposed a draft Convention as an alternative to the Budapest Convention, and in 2019, the U.N. voted to advance the Russian-drafted resolution – with the support of Russia, China, North Korea, Belarus, Syria, and Venezuela, among others. At the time, the United States and key allies urged opposition to the resolution, with one European official declaring “the big picture is that Russia and China are seeking to establish a set of global norms that support their view of how the internet and information should be controlled.” Nevertheless, the resolution was adopted and in August 2024, after years of negotiation, the Convention was adopted by its drafting committee. The Convention is currently on the agenda of the Third Committee of the General Assembly and is expected to be put to a vote before the UNGA as early as December.

We recognize that defending human rights and core principles of internet freedom is not easy. Russia, China and other regimes opposed to democratic freedoms are always working to create international legitimacy for their actions and worldview. The administration's efforts to navigate this complex, consensus-driven process to secure language encouraging countries to uphold their obligations under international human rights law are commendable. Unfortunately, these efforts – while laudable – are insufficient to fix fundamental flaws in the Convention. As currently

drafted, the Convention remains a serious threat to privacy, security, freedom of expression, and artificial intelligence (AI) safety. Specifically, our concerns relate to:

- *Privacy and Surveillance*: Under the proposed Convention, countries are required to adopt laws that allow their authorities to force any person or company to facilitate access to computer systems or stored electronic data. The Office of the U.N. High Commissioner for Human Rights has warned that the Convention could promote surveillance without judicial authorization and directly threaten the global availability of encrypted communications and encrypted services. Encryption provides a lifeline to human rights defenders, journalists, and marginalized or vulnerable people living under authoritarian regimes. Undermining encryption threatens the safety and security of American citizens in the United States and abroad. While the Convention does include certain limited safeguards, those safeguards are inadequate because they exclude explicit requirements for the principles of legality, necessity, and non-discrimination, and instead allow significant deference to domestic laws. In Iran, for example, the lack of such requirements could provide international legal cover for the regime's efforts to promote the widespread surveillance and policing of women and girls. Likewise, the Convention compels countries to collect and share private internet user data with other countries regarding a wide range of crimes. Again, safeguards are present but limited, with nothing to prevent the sharing of data collected under abusive methods, legitimizing dangerous collaboration between authoritarian regimes.
- *Censorship and Freedom of Expression*: Russia, China, Iran, and other authoritarian regimes have long endeavored to leverage government control over the internet and internet-enabled applications to stifle dissent and undermine the freedom of the press. The Convention offers legitimacy to these regimes through an expansive definition of cybercrime that covers not just cyber-dependent offenses, but also a wide range of offenses that may have little or nothing to do with digital technology. The lack of clarity on what can be considered a cybercrime under the Convention introduces the threat that free expression and peaceful assembly will be further criminalized by countries under the guise of preventing cybercrime. This risk is particularly acute, as again the Convention provides for deference to domestic laws and legal frameworks. This deference is highly problematic in the context of this Convention. In Russia, for example, laws criminalize insulting the state, spreading "false news," and using social media to share information on corruption. In China, counter-espionage laws have been expanded to allow for arbitrary enforcement against journalists for routine newsgathering. The lack of specific safeguards against antidemocratic laws and practices will undermine international norms regarding free expression and provide cover for authoritarian regimes to carry out unjustified censorship campaigns.
- *Cybersecurity*: The Convention's articles regarding "illegal access" require countries to criminalize accessing computer systems without permission, but fail to explicitly include good-faith security research exceptions, putting security researchers and journalists at risk of being criminally prosecuted for their work identifying and reporting on vulnerabilities. Without this important work, authoritarian regimes and non-state actors could find it easier to exploit vulnerabilities to breach sensitive data sets and spread malware, making internet users in the United States and around the world decidedly less

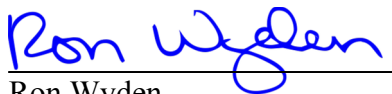
safe. In 2022, the Department of Justice adopted guidelines making clear that good faith security research should not be charged by federal prosecutors, recognizing that “computer security research is a key driver of improved cybersecurity.” We agree.

- *AI Safety and Innovation:* The United States leads the world in the safe development of AI, and continuing to do so is critical to American economic and national security. Yet the Convention’s lack of a good-faith exception for security research, or a requirement for malicious or fraudulent intent for unauthorized access crimes, contradicts the United States’s stated values for AI safety. For example, President Biden’s 2023 Executive Order on AI endorses “red-teaming,” where researchers hack or simulate attacks to identify problems in AI models, like harmful outputs or potential risks of models leaking sensitive or private information. The Executive Order also emphasizes the urgent need for global cooperation on AI safety. For large language models in particular, researchers need models to be tested in different languages and within different cultural contexts to appropriately mitigate harms. The Convention’s lack of protections for AI research risks chilling vital input for model development from a diverse set of researchers, as the President has endorsed through the Executive Order, and could generally result in shrinking global investment in AI safety.

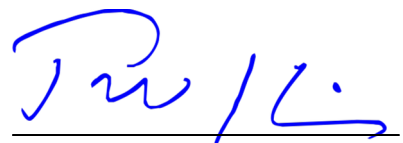
As the UNGA considers the Convention, the United States must not align itself with repressive regimes by supporting a Convention that undermines human rights and U.S. interests. Instead, the United States should lead the charge at the U.N., with allies and partners, for a more balanced and rights-respecting approach to cybercrime. Upholding the values of freedom and human rights is essential not only for U.S. global standing but also for the protection of vulnerable communities worldwide.

Thank you for your attention to this urgent matter.

Sincerely,



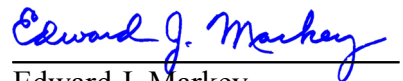
Ron Wyden
United States Senator



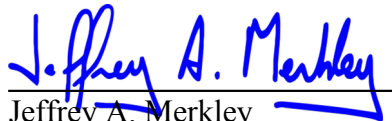
Tim Kaine
United States Senator

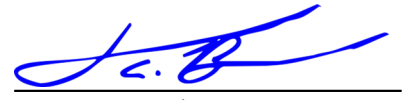


Chris Van Hollen
United States Senator



Edward J. Markey
United States Senator


Jeffrey A. Merkley
United States Senator


Cory A. Booker
United States Senator