

[ADRN Issue Briefing]

Perils of the UN Cybercrime Convention to Free Speech and Privacy: A Global Cartel of Governments for More Power and Data

Kyung Sin Park (Korea University; Open Net)

The United Nations (UN) Cybercrime Convention, if it becomes effective, will be a multilateral treaty whereby State parties *obligate* themselves to (1) criminalize not just certain cyber-attack-like conduct but also certain cyber-enabled conduct under their respective domestic laws (i.e., regulate them as “cybercrimes”); (2) collect, record, seize, and force others to preserve electronic data in the investigation of any and all crimes in various methods that the State parties were previously not obligated to implement under any international law; and (3) share the thus acquired data with one another to facilitate the investigations of the cybercrimes or “serious crimes”. As one of the few norms compelling governments worldwide to strengthen their restrictions on individuals’ conduct and their ability to spy on their subjects, human rights concerns abound. This new international treaty poses perils to free expression and privacy. Some of the conduct required to be criminalized may include legitimate speeches; State surveillance is now made an international obligation without a clear obligation to safeguard privacy; and the inter-State sharing of data will not only double or triple the magnitude of privacy infringements, but it will also bypass existing privacy safeguards such as the warrant requirement of proper constitutional quality. Accordingly, this new treaty requires serious amendments if it is to be ratified in the future.

Risk to Free Expression:

“What Is Criminalized Offline Should Be Criminalized Online Also?”¹

First of all, any mandate to criminalize certain cyber conduct will inevitably impinge upon freedom of speech. This is because “cyber conduct,” by definition, involves transmission and reception of messages, which constitute speech. Cybercrime treaties are the product of realizations that as people’s lives depend profoundly on the internet, some types of speech or cyber activities can become unilaterally harmful, and therefore need international cooperation in preventing through process of law. Therefore, the draft Convention, like its predecessor Budapest Convention, obligates the State parties to restrict certain forms of expression or cyber conduct by obligating them to criminalize them. Then, in doing so, it is important not to cross the lines between those unilaterally harmful speeches like cyberattacks and ordinary speeches protected by human rights.

¹ This famous line is a play on the words of the oft-repeated resolutions of the United National Human Rights Council since 2012. The original reads: “What is protected offline should be protected online also.”

The current list of these mandatory crimes seems innocuous on the surface. The first seven offenses are cyber-attack type activities lifted from the Budapest Convention. These include unauthorized access, unauthorized interception, data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud. Others are ‘cyber-enabled’ crimes: Child pornography related offenses are also lifted from the Budapest Convention and the three new ones of solicitation or grooming of minors, dissemination of non-consensual intimate images, and money laundering do not seem controversial.

However, the definition of “fraud” in Article 13 has been expanded in a manner that allows it to be abused to create and enforce the “false news” crimes. These have been used as pretexts for authoritarian governments to suppress dissident journalists and human rights defenders. It requires criminalizing *“the causing of a loss property to another person by means of ... any deception as to factual circumstances made using [a computer system] [an information and communications technology device] that causes a person to do or omit to do anything which that person would not otherwise do or omit to do”*. The notions of ‘deception’ and ‘omission to do anything’ are extremely vague and could potentially be used to criminalize and prosecute legitimate activities. The requirement of a loss of property to another person can be satisfied if anyone suffers from financial harm. For instance, a human rights defender who initiates an online consumer boycott of a company that supports a military dictatorship could be easily prosecuted under this crime if the law enforcement can identify minor factual inaccuracies in the boycott literature.

Additionally, the concept of “interference with an information and communication technology system” under Article 10 of the draft Convention, inherited from the Budapest Convention, has the potential to impede the utilization of technology by human rights defenders. For example, in South Korea, a political activist was arrested and indicted for commenting and liking *en masse* in an apparent campaign to support certain political views by exaggerating popular support for them (Park 2019). What set him apart from other political activists was that he used other peoples’ cyber identities though not without consent and automated the generation of comments and likes through software. He was charged with the decades-old crime under the domestic law of “interference with business by means of illegitimate use of information and communication networks,” which has been the main provision used for punishing cyber hacking. However, the right to anonymous communication, as affirmed by the 2012 Korean Constitutional Court’s decision on the Internet Real Name Law and the 1995 US Supreme Court case *Terry v. Ohio*, allows people to assume fictitious or pseudonymous identities. To be sure, the real owners of the identities have not complained of any injury or lack of consent. The fact that he used automation should not be the basis of illegitimacy. Automating the exercise of freedom of speech should not be considered a crime, though it may be regarded as impolite and raucous, similar to the use of amplifiers in a classroom. If such actions are deemed criminal, then the creation of a website would also be considered a crime. Such automated commenting is different from hacking which does undermine the ordinary functioning of the network.

Extrapolating from the above example, we can see how the Convention’s definition of cyber hacking can be broadened to suppress legitimate political activities that rely on digital technology. The mandate to criminalize it in the draft Convention, just as the Budapest Convention, should be accompanied with some safeguards against becoming a tool for suppressing democracy.

Furthermore, as the original purpose of the cybercrime treaties was to protect the integrity of information and communication system, it is paradoxical that neither the Budapest Convention nor

the new draft Convention mandates exceptions to legitimate security researchers (i.e., white hat hackers). The draft Convention makes only passing remarks to the contributions of these researchers in the section discussion “Preventive Measures” against further cybercrimes, acknowledging their significant role in enhancing system integrity.

What is even more problematic is that Article 4 of the draft Convention requires the State parties to extend their existing criminal laws, established under international treaties, to the online counterparts. It seems to suggest a principle of equivalence, whereby “what is criminalized offline should be criminalized online also”. For instance, a law criminalizing threats of physical violence may be applied to a dissident activist who uses aggressive language against the rulers of his country through an online posting (Freedom Online Coalition Advisory Network 2024). The draft Convention attempts to address this concern with Article 6 which requires ‘consistency’ with international human rights law and barring any interpretation “as permitting suppression of human rights or fundamental freedoms, including ... freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association.” It remains to be seen whether this vague reference is sufficient. Although the majority of European governments appear satisfied (The Netherlands’ Ministry of Foreign Affairs 2024), it is not surprising that the incumbents will agree to give themselves more power over (and more data about! – see next sections) their subjects than the people to be restricted and surveilled would like to allow.

Surveillance Now Made an International Law Obligation: The Dangers of a Surveillance Treaty in Absence of a Privacy Treaty

Secondly, the State parties, previously not obligated to conduct surveillance, will now be required to conduct surveillance as a matter of duty under this new international law. The six mandatory surveillance measures are as follows: expedited preservation of stored electronic data, expedited preservation and partial disclosure of traffic data (as part of preserved stored electronic data), production order, search and seizure of stored electronic data, real-time collection of traffic data, and interception of content data (heretofore, the same as the Budapest Convention).² For instance, no state was previously obliged to enact legislation authorizing the interception of content data, a requirement now enshrined in the Convention. Such duty arises not just with cyber-attack crimes or ‘cyber enabled’ crimes but in all crimes. What is jarring, there is currently no international treaty protecting privacy other than the International Covenant on Civil and Political Rights (ICCPR), and its Article 17 on privacy is very brief and has not been fully operationalized in restraining the world governments’ appetite for surveillance on their own citizens or others’ citizens for that matter. In contrast, ICCPR’s Article 19 on freedom of expression on which the United Nations Human Rights Committee, the body charged with monitoring ICCPR State Parties’ compliance, has issued a general comment (General Comment 34) in 2011, relatively recently, after absorbing the lessons of the digital age since the arrival of the internet in the early 1990s. The UN General Assembly has also appointed and benefited from the services of the Special Rapporteur on Freedom of Opinion and Expression, who has upgraded and concretized the free speech norms for decades through their thematic and state visit reports. The specific rules on defamation, internet shutdowns, net neutrality, broadcasting,

² There are other mandatory measures newly added to the Convention such as confiscation of crime proceeds, witness protection, and victims’ assistance, which I will not discuss here.

intermediary liability exemption, were promulgated for the specific application in various free speech disputes around the world.

However, there has been comparatively little action on the issue of privacy. Data protection laws have become popular and spread to an ever-growing number of countries, some of them have created arguably the only international treaty on privacy, namely Convention 108/108+. However, domestic and international data protection norms typically include significant exceptions for government agency functions such as surveillance and statute-authorized data processing, which renders them ineffective for regulating data collection by governments for criminal investigation purposes. The proponents of the draft Convention appear to be unaware of the implications of a treaty that encourages, if not requires, global governments to restrict people's privacy in the absence of a countervailing treaty that protects and promotes it.

All of this across-the-board erosion of privacy may be justifiable if the cybercrime treaty is limited to serious crimes of some universal import. Unfortunately, however, both in the Budapest Convention and the new draft Convention, the mandate for the surveillance measures applies to *all crimes*. The 'serious crimes' limitation applies only to international sharing of data, to be discussed later. Although these mandatory surveillance measures are to be moderated by the existing domestic laws (such as constitutional law protecting the rights of the surveilled) under Article 24 paragraph 1, there is no guarantee that these domestic laws operate in the direction promoting privacy. While the Budapest Convention explicitly references the ICCPR and other human rights treaties that these domestic laws must align with, the draft Convention merely mentions "international human rights law."

Fortunately, Article 24, paragraph 2 does (as the Budapest Convention's comparable provision does) includes "judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and duration of such power or procedure," which corresponds to judicial warrants in many democracies. One may have hoped that many countries where surveillance has been conducted without judicial approval may be now obligated to implement judicial approval requirements for future surveillance. However, Article 24, paragraph 2 snuffs that hope out by introducing a limitation: "[i]n accordance with and pursuant to the domestic law of each State Party."³ Of course, the domestic law is supposed to "provide for the protection of human rights in accordance with its obligations under international human rights law" under paragraph 1 but as we discussed before, it suffers from lack of specificity. In the absence of a specific treaty that requires judicial approval for surveillance, the provisions of Article 24 paragraph 2 are rendered ineffectual.

That these surveillance measures, though already administered by many governments voluntarily, become an obligation under international law is concerning when the risk of moral hazard among the incumbent governments quick to agree to give themselves more data has not been hedged by a countervailing treaty protecting privacy.

³ *Article 24. Conditions and safeguards*

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of proportionality.
2. In accordance with and pursuant to the domestic law of each State Party, such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, include, inter alia, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure. (emphasis added)

Surveillance Doubled-up and Unvetted: We Should Have a Right to Have Warrants to Search Us Reviewed by Judges Obligated to Respect Our Privacy

Thirdly, the sharing of the fruits of surveillance among the State parties naturally derogates from privacy of the person surveilled. If one law enforcement agency conducts a search and seizure of an individual and shares the resulting information with another law enforcement agency, it is tantamount to two distinct agencies conducting their respective surveillance activities upon that individual. Such a doubling-up of restriction on privacy can occur in the same way when the nationalities of the two law enforcement agencies are different, as in a typical scenario contemplated by the draft Convention.

International human rights law and constitutional criminal procedure focus on the point where private data crosses the boundary between a person's private domain and the law enforcement but not so much on what happens to the data afterwards. Data protection law has the potential of regulating the use or transfer of data obtained as a result of surveillance activities. However, this can be circumvented by any statute that authorizes such sharing, as most data protection norms make exceptions to statutory mandates or use for public agency functions. Now the draft Convention requires the sharing of acquired data among the State parties.

Such data sharing not only quantitatively erodes the privacy interest of the surveilled, since more than one State parties will now have access to the data, but suffers from an important defect of constitutional quality: the acquisition of the data by the *receiving* State party is not vetted by anyone for the balance between the need for such surveillance and the privacy of the individual subject to it. This implies that the receiving State party may be obtaining the information for reasons that do not justify the privacy restriction that the surveilled individual has suffered. A more diabolical scenario is when a dissident journalist living in State A is searched and seized on his mail server located in State B, by the latter's law enforcement for, for example, copyright infringement, and State B shares the results of search and seizure with State A, which then may use the information for investigation of his political crime at home. In this scenario, there was no neutral magistrate who weighs and justifies the privacy violation against the necessity and proportionality of the criminal investigation by State A. State B's judge, with absolutely no constitutional duty to respect the privacy of the journalist living in State A, will have only weighed the privacy of the mail server operator against State B's need to investigate the copyright infringement. The end result is that the journalist's privacy will have been restricted without proper safeguards. Article 24's calls for "judicial independent review" as a safeguard for human rights becomes an empty cry.

The Budapest Convention dilutes such risk by allowing the State parties to refuse data transfer if the requesting State parties are requiring it for investigation of "political offence". There is no such limitation in the draft Convention. The only limitation is that it be one of the cybercrimes defined in the draft Convention or "serious crimes (crimes carrying more than 4 years in imprisonment)." This means that, if a State party that punishes homosexuality or political dissent by imprisonment of 4 years makes a data request, the responding State is under a duty to cooperate under the draft Convention. Dual criminality (i.e., the requirement that the crime for which the data request is made must be also a crime in the responding state), if it were a mandatory condition for such data sharing, would have diluted the aforesaid privacy harm but it was made optional. The proponents of the draft Convention are arguing that the State parties are free to reject data request on the dual

criminality ground or for other reasons. However, such answer may be valid from a perspective of national sovereignty but turns a blind eye to the fact that the sharing of the data itself erodes and hurts the privacy of the person surveilled as demonstrated above, as such refusal is within the discretion of the responding State party. Remember that the person on whom the data sharing takes place has never been included in what might turn out to be a cartelization among incumbent governments seeking more data! ■

References

- Freedom Online Coalition Advisory Network. 2024. “Proactive Advice: UN Convention Against Cybercrime.” September 16. <https://freedomonlinecoalition.com/foc-advisory-network-proactive-advice-un-convention-against-cybercrime/?hilite=UN+Convention+Against+Cybercrime> (Accessed December 16, 2024)
- Park, Kyung-sin. 2019. “Politics and Internet is an Inevitably Explosive Mix: the case of online opinion rigging.” Open Net. April 13. <http://old.opennetkorea.org/en/wp/2540> (Accessed December 16, 2024)
- The Netherlands’ Ministry of Foreign Affairs. 2024. “Freedom Online Coalition Chair’s Response to the FOC-AN’s Proactive Advice on the UN Cybercrime Treaty.”

- **Kyung Sin Park** is a Professor of Korea University Law School and Director of Open Net.

The East Asia Institute takes no institutional position on policy issues and has no affiliation with the Korean government. All statements of fact and expressions of opinion contained in its publications are the sole responsibility of the author or authors.

This program was funded in part by the National Endowment for Democracy (NED).

“Perils of the UN Cybercrime Convention to Free Speech and Privacy:
A Global Cartel of Governments for More Power and Data”

979-11-6617-841-2 95340

Date of Issue: 20 December 2024

Edited by Hansu Park

For inquiries:

Hansu Park, Research Associate

Tel. 82 2 2277 1683 (ext. 204) hspark@eai.or.kr

The East Asia Institute
1, Sajik-ro 7-gil, Jongno-gu, Seoul 03028, Republic of Korea
Phone 82 2 2277 1683 Fax 82 2 2277 1684
Email eai@eai.or.kr Website www.eai.or.kr