Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

REFERENCE:
OL USA 4/2020

19 March 2020

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 34/18.

In this communication, I would like to submit comments concerning the **Eliminating Abusive and Rampant Neglect of Interactive Technologies** ("EARN IT Act of 2020") Bill, introduced in Congress on 5 March 2020, and I would respectfully request that they be shared with the co-sponsors of the legislation.

Few areas of public policy enjoy as much consensus as there is concerning the protection of children from sexual exploitation. The "EARN IT" legislation, on its face, aims to address the particular threat of child sexual abuse material ("CSAM") in online settings, and that is clearly a legitimate objective. Nonetheless, even the most critical public policies must be consistent with domestic and international law.

In the context of domestic American law, a number of civil society organizations based in the United States have raised serious concerns about the legislation. Those concerns are, in the main, rooted in American Constitutional law, in particular the First and Fourth Amendments of the Constitution. Some of the concerns are particularly focused on the potential impact on privacy and expressive rights, including a concern that the legislation would open the door to vulnerabilities to encryption, a foundation of digital security.

While I share such concerns, I wish to focus on U.S. obligations under the International Covenant on Civil and Political Rights ("the Covenant"), ratified by the United States on 8 September 1992. As President George H.W. Bush noted when urging the Senate to approve ratification of the Covenant, the central treaty in international human rights law, it "codifies the essential freedoms people must enjoy in a democratic society."[1] Of most relevance to the EARN IT legislation, Article 17 protects everyone's right to privacy while Article 19 guarantees the freedom of opinion and expression.

Below I provide some preliminary reactions to the legislation based on U.S. obligations under the Covenant. In short, I am concerned that the legislation would open the door to steps by the U.S. Government that would be inconsistent with its obligations under Articles 17 and 19 of the Covenant. I am particularly concerned that the legislation gives excessive discretion to the Department of Justice and others to compel providers to

[1] Senate Exec. Rept. 102-23, March 24, 1992, at page 25.

modify digital security standards or take other action that would effectively weaken encryption. I urge reconsideration of the legislation in keeping with the human rights standards outlined below.

A. The framework of international human rights law

Before describing my specific concerns, I wish to note in brief the applicable rules of human rights law that are of relevance to any consideration of legislation or policies with an impact on privacy or freedom of expression. Those relevant human rights obligations may be found in Articles 17 and 19 of the Covenant. Article 17 specifically protects individuals against "arbitrary or unlawful interference with his or her privacy, family, home or correspondence", providing that "everyone has the right to the protection of the law against such interference or attacks." Article 17 permits interference with the right to privacy only where it is "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant", is in pursuit of "a legitimate aim" and "meet[s] the tests of necessity and proportionality".[2] The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression.[3]

Article 19(1) of the Covenant establishes the right to freedom of opinion without interference; it is not subject to any restriction. Article 19(2) guarantees everyone's right to the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." Article 19 (3) articulates a three-part test requiring that restrictions be provided by law and be necessary to protect the rights or reputations of others, national security or public order, or public health or morals. The Human Rights Committee, the Covenant's monitoring body, has emphasized that these principles, at a minimum, mean the following:

(a) *Provided by law/legality*: Any restriction must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. The "provided by law" standard is widely understood to mean that restrictions must be sufficiently clear, accessible, and predictable, such that they do not provide excessive discretion to public authorities.[4] The assurance of legality should generally involve the oversight of independent judicial authorities.[5]

---

[2] Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism, A/69/397 (23 September 2014), ¶. 30. *See also* High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), ¶ 21 – 30.

[3] See General Assembly resolution 68/167 and Human Rights Council resolutions A/HRC/13/37 (28 December 2009) and A/HRC/20/8 (10 April 2012).

[4] U.N. Human Rights Comm., General Comment No. 34, Freedoms of Opinion and Expression (Art. 19), U.N. Doc. CCPR/C/CG/34 (12 September 2011). ¶ 25.

[5] Human Rights Council, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/HRC/29/32, ¶ 32 ("A/HRC/29/32").

(c) *Legitimacy*: Article 19 (3) imposes specific limits on the interests justifying restrictions. While it is common for States to seek to justify restrictions, the Human Rights Committee has clarified that the burden is on the State to justify any rule that impacts the enjoyment of the right to freedom of expression. While the first of the legitimate grounds for restriction listed in paragraph 3 of Article 19 is that of respect for the rights of others (e.g., the right to be free from physical harm or exploitation), the State must still justify the legality and necessity of measures to meet that objective.

(b) *Necessity and proportionality*: The State has the burden of proving a direct and immediate connection between the expression and the threat. The necessity and proportionality standards ensure that that restrictions "target a specific objective and do not unduly intrude upon the rights of targeted persons."[6] The ensuing interference with third parties' rights must also be limited and justified in the interest supported by the intrusion.[7]

In the context of online expression, my own reporting has found that "States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process" and the aforementioned standards of legality, necessity and legitimacy. States should also refrain from imposing disproportionate and unnecessary sanctions on Internet intermediaries, given their significant chilling effect on freedom of expression.[8] I have also urged States to refrain from adopting models of regulation "where government agencies, rather than judicial authorities, become the arbiters of lawful expression."[9]

B. Key concerns under the draft EARN IT Act

Permit me to address specific provisions of the EARN IT act in order to highlight my concerns in light of U.S. obligations under the Covenant. To be sure, the purpose of the legislation —to address CSAM by creating a National Commission on online child exploitation prevention – is a legitimate objective of law and policy, whether framed as a protection of the rights of children, of public order, or of public health or morals. The pertinent question is whether the legislation would pose risks to fundamental freedoms, in particular privacy and expression, that cannot justified in accordance with the standards of legality and necessity and proportionality outlined above.

Because of the implications of the legislation for encryption – notwithstanding the argument that the legislation would not address the issues – I would like to offer one note about digital security.[10] Restrictions on encryption, as an enabler of the privacy necessary for freedom of expression, must satisfy the requirements of legality, legitimacy, and necessity and proportionality described above. Proposals to impose such restrictions,

[6] *Id*, A/HRC/29/32, ¶ 35 ("A/HRC/29/32"); *See also*, U.N. Human Rights Comm., General Comment No. 27, Freedom of movement (Art. 12), U.N. Doc. CCPR/C/21/Rev.1/Add.9 (2 November 1999)
[7] *Id.*, A/HRC/29/32, ¶ 35.
[8] Human Rights Council, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/HRC/38/35 (6 April 2018), ¶ 66.
[9] *Id.*, ¶ 68
[10] My reporting on encryption and freedom of expression may be found at the report at footnote 7.

particularly given their impact on expression and privacy, should be subject to public comment and *only be adopted, if at all, according to regular legislative process.* Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose right to freedom of expression is subject to restriction. Blanket prohibitions of encryption, for example, plainly fail these conditions, as would vulnerabilities or mandates that render encryption virtually useless. Measures that systematically weaken encryption and digital security more generally, such as backdoors, key escrows, and data localization requirements – all of which may result from demands to monitor – may also interfere with rights to opinion, expression and privacy.

1. **Creation of a National Commission on Online Child Sexual Exploitation Prevention**:

The legislation would establish a 19-member Commission which purpose is to "recommend best practices that providers of interactive computer services may choose to engage in." The "recommendations" are intended to "prevent, reduce and respond to the online sexual exploitation of children"[11] and CSAM online. Its "best practices" recommendations may then be fast-tracked to a vote in each house of Congress (see section 3 below).

Civil society organizations and academic observers have raised concerns about the dominance of members of the law enforcement community, and the likelihood of the Commission adopting "best practices" that could reflect their agenda in an unbalanced way. I am especially concerned that the Commission may operate and make decisions without an expert on privacy who may address, for example, the risks of weakening encryption protections. The inclusion of an expert on cryptography seems to indicate that the Commission would evaluate and possibly weaken encryption standards.

I am concerned that the legislation grants excessive powers to this Commission, which would dictate the parameters for providers to police online speech. The Commission would have the leeway to constrain the features of online services and speech by determining, for example, how people are allowed to communicate and what type/content of discourse should be monitored and eventually censored. In effect, this Commission would be in charge of determining the restrictions on freedom of expression online.

2. **The duties of the Commission**:

The Commission, upon approval of at least 14 of its members, would have to submit the "recommended best practices" to the Attorney General. The proposed legislation states that the Attorney General, "upon agreement with" the heads of DHS and the FTC, shall either approve or deny the "best practices" [Section 4 (b)(1)]. However, it remains unclear if the Attorney General has unilateral approval/denial power, if the majority of the heads of the departments have to approve it, or if it there has to be a

[11] The legislation states "including the enticement, grooming, sex trafficking, and sexual abuse of children" [Section 3 (b)]

consensus among them. The confusion stems, for example, from Section 4 (b)(2) which is directed only to the Attorney General: "[i]n determining whether to approve or deny recommended best practices under paragraph (1), the Attorney General shall consider" the purpose of the Commission and other "relevant considerations".

The proposed legislation includes a list of 11 "matters" that *shall* be addressed by the "recommended best practices." The scope of the matters that could be included in the "best practices" raises serious concerns. For example, some have stated that the Commission could issue a "recommendation" to providers to monitor all communications for CSAM. Compliance with such a recommendation would require that providers build certain vulnerabilities into their encrypted communications systems. Moreover, the legislation does not contemplate warrants or any judicial finding of probable cause in order to undertake such efforts. The structure set up by proposed legislation, paradoxically, might make it even more difficult for prosecutors to hold those responsible accountable.

As mentioned above, any restriction on freedom of expression must comply with the principle of legality. This principle includes the application of strong procedural and judicial safeguards to guarantee the due process rights of any individual whose right to freedom of expression is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction (see part 4).

While combating CSAM online is a legitimate goal, any measure that restrict freedom of expression should be the least serious measure available to safeguard rights and/or other essential legally protected interests. Therefore, among the various options available for reaching the same objective, the State should choose the one that least restricts freedom of expression. For example, in order to address the proliferation of CSAM online, there are other less restrictive ways, such as increasing the number of prosecutors and officials in the Department of Justice that work on these issues, or increasing the number of agents to the already existing Federal Agencies tasked with addressing CSAM. I understand that these and other ideas have already been proposed by other members of Congress.

The legislation also states that in developing best practices, the Commission *shall* consider "[…] (C) the impact on the ability of law enforcement agencies to investigate and prosecute child sexual exploitation and rescue victims; and (D) the current state of technology." [Section 4 (a)(4)]. These "relevant considerations" are particularly problematic given that in many nations, including the United States, law enforcement officers have alleged that encryption hinders their ability to carry out investigations, and therefore, I am concerned that the Commission could decide to undermine the availability of secure end-to-end encryption.

3. **Fast-track legislative authority:**

After the approval by the Attorney General, the best practices are published on the website of the DOJ and the Federal Register. The recommended best practices have to be submitted in their entirety to Congress and a 'covered bill' incorporating them shall be introduced. The covered bill would be fast-tracked to a vote in each house of Congress. If the Attorney General denies the "recommended best practices", she or he would be required to write up the basis for and the reasons that support the denial [Section 4 (b)(3)]. The Commission may resubmit the recommended best practices when (i) they are denied or (ii) a bill that contains the best practices is not enacted under the expedited procedures described.

I am concerned that, contrary to the "provided by law" standard of Article 19(3), the design of this Commission sets up a system for *de facto* adoption of rules that companies should abide by without going through regular Congressional procedure. Moreover, the process seems to delegate the power of determining the requirements of accessing essential protection against liability to the Attorney General.

4. **Earning immunity under Section 230**:

The legislation would amend Section 230 of the US Communications Decency Act, which currently shields online service provider from liability for content that their users post, link to, or transmit using their services. The bill proposes that interactive computer service providers "earn" their liability protection for violations of laws related to CSAM online by either: 1) *certifying* to the Attorney General that it has implemented, and is in compliance with the congressionally-approved "best practices"; or 2) showing that they have "implemented reasonable measures relating to the matters [covered by the bill's provision governing best practices]" [Section 6(a)]. However, the term "reasonable measures" is not explicitly defined, which gives the Commission broad discretion and renders the safe harbor functionally useless for most providers. The bill also criminalizes making a false statement in a certification of "best practices" (a fine and/or up to two-year prison sentence).

The proposed legislation would also lower the standards of evidence required in civil lawsuits under which providers may become responsible for CSAM on their system. "Conduct by a provider of an interactive computer service […] that would violate section 2252 or section 2252A if that section were applied by substituting 'recklessly' for 'knowingly'" [Section 6 (b)]. Currently, providers are liable if they "know" their users are distributing CSAM on their platforms. The proposed EARN IT Act allows for providers to become liable if they "recklessly" provide a service that people use to distribute CSAM. The burden would then be on the provider to show that they followed the best practices or otherwise implemented "reasonable measures".

The modifications to current liability protections to providers and the language that lowered the *mens rea* for civil liability will, in effect, make the "best practices" mandatory requirements. Such rules also involve risks to freedom of expression, putting

significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability. These "recommendations" could end up demanding for quick, automatic removals risking new forms of prior restraint on expression.[12] Moreover, the increased legal liability could disincentivize the use of end-to-end encryption. This not only risks individual users' privacy and freedom of expression, but it could also produce a chilling effect on these rights. Finally, these "recommendations" could also involve the delegation of regulatory functions to private actors which lack basic public tools of accountability. The "complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards."[13]

Governments should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy as stated above. They should refrain from imposing disproportionate sanctions, whether heavy fines or imprisonment, on Internet intermediaries, given their significant chilling effect on freedom of expression.[14] Previous special rapporteurs and I have emphasized that "no one should be held liable for content on the Internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf."[15]

C. Conclusions

In light of the above-mentioned standards and concerns, I am concerned that the legislation, if adopted, would be incompatible with international human rights law. The legislation does not seem necessary or proportionate to achieve the goal of addressing CSAM, nor does it comply with the legality standard. Instead, it threatens the widespread adoption of strong encryption, which is essential for protecting freedom of expression and privacy of those who use the internet. I am also concerned that the legislation confers on select public officials an excessive authority to restrict, censor and punish online expression. I am concerned that it would not only serve as a basis to deter fully legitimate speech, but also that it could serve as a model for far reaching restrictions on vague and discretionary grounds.

I urge that the legislation be modified to meet U.S. obligations under the Covenant and that Congress provide adequate additional time for legislative and public consideration to evaluate revised, or different legislation, if necessary, to address the legitimate aims of protecting against CSAM and its dissemination.

In connection with the above alleged facts and concerns, please refer to the **Annex on Reference to international human rights law** attached to this letter which cites international human rights instruments and standards relevant to these allegations.

---

[12] Human Rights Council, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/HRC/38/35 (6 April 2018), ¶ 17.
[13] *Id.* A/HRC/38/35, ¶ 17
[14] *Id.* ¶ 66
[15] Human Rights Council, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, A/HRC/17/27 (16 May 2011), ¶ 43.

As it is my responsibility, under the mandate provided to me by the Human Rights Council, to seek to clarify all cases brought to my attention, I would be grateful for your observations on the following matters:

1. Please provide any additional information and/or comment(s) you may have on the above-mentioned allegations.

2. Please provide information on the measures taken to ensure the compatibility of the EARN IT act with international human rights standards.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from your Excellency's Government will be made public via the communications reporting website within 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression