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

REFERENCE:
AL IND 31/2018

18 January 2019

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 connection, I would like to bring to the attention of your Excellency's Government information I have received concerning **the Government request to WhatsApp to provide private user information to the authorities**.

According to the information received:

In May 2017, seven individuals were killed in a mob-lynching reportedly prompted by disinformation spread through WhatsApp groups. Similar attacks have continued throughout India. The disinformation has usually targeted individuals who are viewed as outsiders in the community, in most cases because they are from a different area or speak a different language, but also due to their appearance, race, or religion. As of July 2018, it is estimated that there have been over twenty deaths and several more injured tied to disinformation spread through WhatsApp.

On 3 July 2018, the Indian Ministry of Electronics and Information Technology ("MeitY") sent WhatsApp a letter regarding the lynching. It asked the company to "come out with suitable interventions" to "avoid such undesirable eventualities."

That same day, WhatsApp responded with a letter detailing its actions to prevent such abuses in the future. This includes "a new label" "that highlights when a message has been forwarded versus composed by the sender" and various educational initiatives, including educating users on disinformation and instructing law enforcement agencies on how to best use the app.

On 19 July 2018, MeitY sent WhatsApp another letter requesting WhatsApp to "bring in traceability and accountability." Specifically, it stated that when "a request is made by law enforcement" the service needed to have the ability to "ascertain [the] identity of the person(s) from whom the messages originated and through whom it was propagated." MeitY also indicated that if WhatsApp failed to do so, "it may not be out of place to consider the medium [WhatsApp] as an abettor."

On 27 July 2018, WhatsApp responded by outlining new features to stop the spread of disinformation. Specifically, it: added "limits to the forwarding of

messages . . . [to] just five chats at once"; "removed the quick forward button next to media message"; implemented "better protections for users who want to leave groups"; and "established a legal entity in India." WhatsApp refused, however, to collect the requested information, stating that "tracing private messages would undermine the private nature of the app with the potential for serious consequences for free expression".

Though information received suggests that MeitY is still pressing WhatsApp to change its technology to allow for identification of senders, it has yet to respond to WhatsApp's latest letter.

I want to first recognize your Excellency's Government's legitimate objective to protect the right to life, and to protect individuals against acts of violence which have been prompted by the spread of disinformation on WhatsApp. Speech that incites violence may be permissibly regulated subject to the requirements under article 19(3) and article 20(2) of the International Covenant on Civil and Political Rights (ICCPR), acceded to by India on 10 April 1979 . I am concerned, however, that your Excellency's Government's pursuit of user information may impermissibly interfere with article 17 and article 19. For reasons discussed above, WhatsApp's encrypted services play a vital role in promoting freedom of opinion and expression. WhatsApp has over 200 million Indian users and the company reports that people use it in India to have "all kinds of sensitive conversations, including with their doctors, banks, and families." WhatsApp also claims that they are getting reports of "the police using it to discuss investigations, as well as citizens to report crimes." The information that your Excellency's Government is requesting WhatsApp to provide would undermine the benefits and protections the encryption provides. Court-ordered decryption and access to user data, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals and subject to judicial warrant and the protection of due process rights of individuals.

I am also concerned that seeking user data and metadata from WhatsApp is disproportionate as a measure to prevent violence. WhatsApp has implemented several less-intrusive measures to address this issue. These measures include working a large-scale public service campaign to educate users on disinformation, educating police, and changing the functioning of the app itself, such as limiting the number of chats you can forward messages to and fact-checking in app. Since July 2018, there have been no new reports of WhatsApp-driven mob violence. Additionally, in order to obtain the requested information WhatsApp would need to alter the functioning of its app, as it currently does not record much of the information the government is seeking.

I am further concerned that your Excellency's Government's threat to classify WhatsApp as an "abettor" if it refuses to turn over user information when "a request is made by law enforcement agency" is overbroad and lacks sufficient accountability. The requirement fails to specify what, if any, legal procedures and protections any such request would be bound by, suggesting this does not meet the standard of being "provided

by law." Further, it would be forcing WhatsApp to violate its own obligations to "respect human rights" and "avoid infringing on human rights of others" (A/HRC/17/31).

In connection with the above alleged facts and concerns, please also 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 the allegations.

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 comments you may have on the above-mentioned allegations.

2. Please explain what other measures adopted by your Excellency's Government have been used to curb the spread of the disinformation or to identify those responsible for the spread of the disinformation, and if and why those methods have been deemed ineffective.

3. Please explain how the request by your Excellency's Government to obtain user data is in line with article 19(1), given the Special Rapporteur's indication that encryption protect freedom of opinion and given there are no permissible interferences with freedom of opinion.

4. Please explain which laws WhatsApp's actions have violated and how any legal action against WhatsApp would be in line with articles 19(3) and 17(1) of the ICCPR.

5. Please indicate alternative measures considered by the Government which would protect user information from arbitrary search and would enable business enterprises to discharge its responsibility to respect human rights.

I would appreciate receiving a response within 60 days. Passed this delay, this communication and any response received from your Excellency's Government will be made public via the communications reporting website. 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

Annex
Reference to international human rights law

In light of the above allegations, we wish to stress the obligation of your Excellency's Government to respect, protect and promote the right to freedom of opinion and expression under article 19 and the right to privacy under article 17 of the International Covenant on Civil and Political Rights (ICCPR), acceded to by India on 10 April 1979.

In particular, article 19(1) of the ICCPR establishes the right to freedom of opinion without interference. Article 19(2) protects the right to "seek, receive and impart information 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." Under article 19(3), restrictions on the right to freedom of expression must meet a three-part test. That is, restrictions must be "provided by law", and necessary for "respect of the rights or reputations of others" or "for the protection of national security or of public order (ordre public), or of public health and morals." General comment No. 34 of the Human Rights Committee states that "a law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution" (CCPR/C/GC/34).

When a State does invoke article 19(3), the Committee has required that it specifically show it "invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat" (CCPR/C/GC/34). Notably, the concept of proportionality requires, under General Comment 34, that restrictive measures be "appropriate to achieve their protective function," be the "least intrusive instrument," and must be "proportionate to the interest to be protected."

Article 17 of the ICCPR provides in relevant part that "no one shall be subjected to arbitrary or unlawful interference with his privacy." The permissible limitations on the right to privacy should be read strictly and, when freedom of expression rights are implicated, they must also meet article 19(3) standards (A/HRC/29/32). Moreover, privacy and freedom of expression are interlinked and mutually dependent (A/HRC/23/40). In addition, the General Assembly, the United Nations High Commissioner for Human Rights, and Special Procedures mandate holders have held that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression (see General Assembly resolution 68/167, A/HRC/13/37, Human Rights Council resolution 20/8, and A/HRC/29/32).

The Special Rapporteur on the right to freedom of expression has also recognized the special role that encryption and anonymity plays in protecting privacy and thus facilitating the right to freedom of opinion and expression. Encryption protects

individuals “right to seek, receive, and impart information and ideas” “where they are otherwise denied,” particularly with political expression and scientific endeavors (A/HRC/29/32). It “provides security” and is “especially useful for the development and sharing of opinions, which often occur through online correspondences” (A/HRC/29/32). It further protects freedom of expression rights on a global level by enabling people to avoid “States [that] filter or black data on the basis of keywords” thus allowing “information to flow across borders” (A/HRC/29/32). The importance of encryption extends to metadata because metadata “may give an insight into an individual’s behavior, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication” (A/HRC/27/37).

I also wish to draw attention to duty of States, in line with the UN Guiding Principles on Business and Human Rights endorsed in 2011 by the Human Rights Council in its resolution (A/HRC/RES/17/31), to ensure that laws and policies governing the operation of business enterprises do not constrain but enable business respect for human rights (Guiding Principle 3).