



UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion & Expression Call for Inputs: HRC 47th Session Report on Disinformation

16 February 2021

Introduction

Access Now welcomes this opportunity to provide relevant information to the United Nations (U.N.) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (the Special Rapporteur) to inform the Special Rapporteur's report to be presented at the 47th session of the Human Rights Council on disinformation.¹ As an ECOSOC accredited organisation, Access Now routinely engages with U.N. Special Procedures in support of our mission to extend and defend digital rights of users at risk around the world.²

Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of human rights. Access Now works to defend and extend the digital rights of users at risk around the world through policy, advocacy, technology support, grants, legal interventions, and global convenings like RightsCon.

Call for Input

Access Now is pleased to provide input on the Special Rapporteur's thematic report by offering a digital perspective. The submission focuses on three main themes I) amplification of disinformation online, (II) disproportionate legal measures to fight COVID19 disinformation and (III) disinformation in the context of internet shutdowns. Each thematic section is accompanied with case studies collected from our regional policy and advocacy efforts across the globe. It is important to note that while this submission draws upon examples from various regions worldwide, these examples are non-exhaustive. We recognize that further research and data is required to take into account intersecting structures of oppression, including the situations of transgender people, those with non-binary gender identities, and gender non-conforming people, in addition to individuals' various intersecting identities including, but not limited to, race, ethnicity, sexual orientation, disability, class, language, religion, age, citizenship, and family status.³ We encourage the Special Rapporteur to reinforce and build upon the previous efforts of the former mandate holder, David Kaye, particularly addressing disinformation online such as the regulation of user-generated online content.⁴

¹ OHCHR, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, [Report on disinformation](#), 2021.

² Access Now, [About Us](#), 2021.

³ *Digital Media and the Politics of Transformation in the Arab World and Asia*, Ed. by Carola Richter, Anna Antonakis, Cilja Harders, Springer VS, 12 March 2018, at page 143.

⁴ U.N. Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/38/35, 6 April 2018 available at <https://freedex.org/a-human-rights-approach-to-platform-content-regulation/>

I. Amplification of disinformation online

In our 2018 joint report ‘Informing the disinformation debate’, we underlined the importance to distinguish between manipulative business models of large online platforms, their role and economic interests behind the spreading of dis/misinformation **from state-led “hybrid threats” such as cyber attacks and disinformation campaigns.**⁵ Because large online platforms with economic dominance harvest an unprecedented amount of personal data, they are able to boost the engagement of their users and **derive profit by prioritizing or quantifying the popularity of certain types of sensational content, including disinformation.** Their dominant position also enables them to control the online public sphere, while deepening **huge power asymmetries** between them and their users. In the hands of major players, the acts of content moderation and content curation have become a commodity from which platforms generate profit.⁶

Large online platforms have dominant positions in particular markets, and **use content recommendation systems to disseminate content, determining what content is recommended and how.** This provides them with a position of great power and influence. Given the enormous quantity of content being shared on online platforms, private actors have chosen to rely on automation to decide what content will be made visible to whom. The automated decision-making underlying this process of content governance is based on online targeting systems.⁷ **Online targeting lies at the core of data harvesting platforms and it shapes users’ online experience.** Online targeting leverages user profiles and allows large platforms to try to determine and speculate on people’s personal preferences and behaviours.

Recent research findings reveal that **large online platforms and their content recommendation systems can contribute to the polarisation of opinions and attitudes online.** At the same time, it must be noted that several conditions have to be fulfilled for algorithmic filtering to be effective in causing polarization. For instance, an important factor is the predisposition and political attitude of especially those users who are already at the edges of the political spectrum.⁸ Therefore, it cannot be simply assumed that algorithms are capable of polarising society on their own, though attempts to manipulate content curation to drive engagement have been clearly documented. Since **controversial issues** in particular generate user engagement, these issues are more likely to be highly ranked by algorithms and thereby more likely to be visible to a larger audience on social media.⁹ Content recommendation is crucial for the growth and dominance of large platforms, and lies at the heart of their business models. At the same time, their dominant position guarantees them significant

⁵ Access Now, Civil Liberties Union for Europe & European Digital Rights (EDRI), [Informing the “Disinformation” Debate](#), 18 October 2018.

⁶ Gillespie, T. [Custodians of the internet](#). 2018.

⁷ For more information about harmful methods of online targeting, please consult Access Now, [Raising the alarm: online tracking harms human rights](#), 2020.

⁸ Birgit Stark, Daniel Stegmann, [Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse](#). 2020.

⁹ *Ibid.*

quasi-regulatory powers over users and their rights. Or in the words of Gillespie, recommendation systems are "a key logic governing the flows of information on which we depend."¹⁰

While we welcome scrutiny of lawmakers around the globe into the platforms' market dominance, their control over public spheres, and their data-harvesting manipulative business models – all highly problematic to users' human rights – not every regulatory proposal meets the criteria of the international human rights framework and principles of the rule of law. While regulation that establishes a set of procedural safeguards for large online platforms can play an important role in establishing meaningful transparency and robust accountability mechanisms, new frameworks may also impose serious risks of human rights abuse if they incentive platforms to act against lawful speech.

a) Example of national legislative proposals targeting the amplification of potentially harmful and illegal content online

We welcome that some States have recognised the importance to focus on how content is being distributed by platforms and its large societal impact. However, we caution lawmakers around the globe that regulating amplification can have serious negative consequences on the right to free expression and information online. For instance, the Protecting Americans from Dangerous Algorithms bill (PADAA) was introduced by representatives Malinowski and Eshoo in 2021 as a reaction to the U.S. Capitol riots incited by the former president. PADAA is the first, but probably not last, proposal coming for the U.S. that seeks to restrict platforms' "amplification of harmful speech."¹¹

These types of proposals can undermine human rights, and they demonstrate the damaging impact on the rights of free expression and access to information caused by the prevailing pattern of platform regulation. The proposed bill imposes liability on platforms for amplifying not only unlawful content but also for amplifying users' accounts, their affiliation and group pages. Importantly, **lawful speech would be seriously impacted as well because the visibility would be decreased not only for a particular piece of content but for everything expressed by a particular speaker or within a particular group.** Further, this approach of mandating action against accounts and group webpages carries a serious risk of discrimination to underrepresented groups.¹²

II. Disproportionate legal measures to fight COVID19 disinformation

The global health crisis has prompted many governments around the world to take hasty action in pursuit of an effective response to the spread of misinformation and disinformation on the internet and via traditional media. Yet history has shown that hastily crafted legal or policy measures presented as a silver-bullet solution to a national emergency can create an environment of legal

¹⁰ Gillespie, T. [Custodians of the internet](#) 2018.

¹¹ Daphne Keller, [One Law, Six Hurdles: Congress's First Attempt to Regulate Speech Amplification in PADAA](#), The Center for Internet and Society, 1 February 2021.

¹² Daphne Keller, [One Law, Six Hurdles: Congress's First Attempt to Regulate Speech Amplification in PADAA](#), The Center for Internet and Society, 1 February 2021.

uncertainty and enable ongoing human rights abuses. While governments' concerns about national public health and safety are legitimate, any adopted measures for dealing with disinformation may restrict access to information and freedom of expression, and therefore must be proportionate and necessary, and meet a legitimate aim.

We are seeing broadly formulated laws to address COVID-19-related “false news” or “propaganda” to serve as a justification to suppress dissent and criticism of state response to global pandemic. Multiple examples from across the world show states leveraging criminal-law measures to target journalists or healthcare workers who have sought to share important information or criticize governments for their lack of adequate response to the COVID-19 crisis.

a) Russia case study: criminalisation of “false” information about COVID-19

In March 2019, Russia introduced legislation that imposes administrative penalties and **allows blocking of websites without a court order for “dissemination of knowingly false publicly significant information” that “threatens life or health of citizens, property, public order.”**¹³ The law has been used against human rights defenders, environmental activists, and journalists.¹⁴

In the wake of the pandemic, Russia passed additional legislative amendments that increase penalties for “fake news,” making spreading false information about COVID-19 a criminal offense.¹⁵ Thus, a new Criminal Code Article 207.1 makes it a criminal offense to “publicly disseminate disguised as truthful knowingly false information about circumstances threatening life and safety of citizens.” The offence is punishable by fines of up to 700,000 rubles (\$9,000), mandatory labor, or restriction of liberty for up to three years. The new Article 207.2 criminalizes “public dissemination of knowingly false information of public importance” if it leads to death or other “grave consequences.” It will be punishable by up to 2 million rubles (\$26,000), mandatory labor, or up to five years of imprisonment. **Russian authorities have already fined dozens of individuals, opened criminal investigations, and blocked hundreds of websites for spreading “false” COVID-19 information.**¹⁶

b) MENA region case study: national disproportionate criminal legislation combatting disinformation and “fake news”

In March 2020, a member of the Tunisian parliament proposed **a draft law to combat disinformation during the COVID-19 crisis, on the pretext of fighting “fake news” and controlling the flow of**

¹³ [Федеральный закон от 18.03.2019 № 27-ФЗ](#) "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях," 2019; [Федеральный закон от 18.03.2019 № 31-ФЗ](#) "О внесении изменений в статью 15-3 Федерального закона "Об информации, информационных технологиях и о защите информации," 2019.

¹⁴ Amnesty International, [Russian Federation: “Fake news” bill prompted by COVID-19 threatens freedom of expression](#), 2020.

¹⁵ The Moscow Times, [Russia Bans ‘Discussions’ of Fake Coronavirus News](#), 2020; [Федеральный закон от 01.04.2020 № 100-ФЗ](#) "О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации," 2020.

¹⁶ The Moscow Times, [Russia Bans ‘Discussions’ of Fake Coronavirus News](#), 2020; Meduza, [На россиян начали заводить уголовные дела по новой статье о фейках про коронавирус. Мы спросили у нескольких фигурантов таких дел, что происходит](#), 2020.

information on social media platforms that could impact “national security and order.” The proposal, which was tabled in secrecy and without public consultation during the state of emergency in Tunisia, imposed a prison sentence up to two years and a disproportionate fine of 20,000 Tunisian dinars for its violation. The draft law sought to criminalize disinformation or misinformation on social media platforms, while conflating terms such as online defamation and “fake news”. The vague terminology could be easily used against journalistic reporting, political opponents, bloggers and activists critical about governmental policies or officials.¹⁷ With the swift reaction of Tunisian civil society, Access Now, and other groups, the bill was successfully stopped in its tracks.

Similar attempt was observed in Morocco **where the health emergency was exploited to criminalize “fake news” and disinformation through passing repressive legislation.**¹⁸ The draft law punishes “anyone who deliberately uses social networks, open broadcast networks or similar networks to publish or promote electronic content containing false information” with imprisonment between 3 months to 2 years or a fine of 1,000 to 5,000 dirhams (roughly between 111 and 550 USD), or both.

In other countries, such as the case in Jordan and Palestine, governments took a securitized approach to tackling spread of disinformation during the COVID-19 pandemic. **Those who were suspected of spreading disinformation publicly on social media and in private chat groups were immediately arrested by security forces or the police.** In Jordan, the government issued on 15 April 2020, a defence decree which prohibits citizens from publishing, republishing or sharing news or information on the coronavirus virus that might cause panic and fear among citizens.¹⁹ A number of citizens, including journalists, were detained as a result.²⁰

Activists, journalists and human rights defenders have been the primary target for state and non-state orchestrated disinformation and smear campaigns. Egyptian human rights activist, and the sister of jailed activist Alaa Abdul Fatah, Sanaa Seif was arrested on June 23, 2020 on charges of spreading fake news, inciting to terrorism, and misuse of social media.²¹

III. Disinformation in the context of Internet Shutdowns

We see again and again governments using “fake news” and disinformation as an excuse to shut down the internet and leave their populations in the dark. For instance, in a recent lawsuit, the government of Indonesia argued that it shut down the internet in 2019 in order to prevent the spread of fake news in the midst of protests against state violence in the provinces of Papua and West Papua.²² **The**

¹⁷ Access Now, [Tunisia’s Parliament on COVID-19: an initiative to fight disinformation or an opportunity to violate fundamental rights?](#), 2020.

¹⁸ Article 19, [Morocco: Government must fully withdraw draft law on social media](#), 10 July 2020.

¹⁹ Prime Minister of Jordan, [Tweet on Twitter](#), 15 April 2020.

²⁰ Human Rights Watch, [Jordan: Free Speech Threats Under COVID-19 Response: New Penalties for ‘Causing Panic’ About Pandemic](#), 5 May 2020.

²¹ Access Now, [Sanaa Seif arrested in front of Prosecutor-General’s office by plainclothes security forces](#), 23 June 2020.

²² Access Now, [Court rules the internet shutdowns in Papua and West Papua were illegal](#), 2020.

Jakarta court, however, rejected the government’s position, ruling that internet shutdowns were “a violation of the law by government bodies or officials.”²³

According to the #KeepItOn coalition, while governments often insist that they shut down the internet to stop the spread of “fake news, hate speech, or incendiary or violence-inciting content, the reality on the ground shows that **the true reasons for these shutdowns are elections, protests, and political instability that those governments would like to hide or suppress.**²⁴ Ironically, **governments are also often the ones responsible for much of the disinformation content** that they are supposedly trying to suppress through shutdowns.²⁵

Shutting down the internet only helps disinformation and “fake news” to proliferate as it eliminates legitimate sources of alternative and up to date information. This is even more important during the COVID-19 pandemic. As the world grappled with how to deal with misleading information about the pandemic, its remedies, origins, and other information, access to the internet, in addition to other media sources, was more important than ever to help people get the right information at the right time.

a) Myanmar case study: Nationwide Internet shutdown claims to fight against circulation of “fake news”

In February 2021, national military forces in Myanmar seized power during a coup d'etat, detaining State counsellor Aung San Suu Kyi and other democratically elected leaders. A few days later, the Myanmar Ministry of Transport and Communications (MoTC) issued a directive ordering all mobile operators, internet service providers and international gateways to temporarily shut down the data network in Myanmar.²⁶ **The directive cited a legal basis in Myanmar’s Telecommunication Law, and referenced circulation of fake news, stability of the nation and interest of the public as justification of the order.**²⁷

Access Now has been working closely with local partners and concerned organizations across the world, and although the Myanmar situation is constantly changing, a number of key disruptions can be confirmed by the #KeepItOn community:²⁸ The arbitrary timing, scope, and duration of these shutdowns disprove the claim that the disruptions aim to stop the spread of disinformation.

b) Sri Lanka case study: blocking social media platforms as a response to national emergency

²³ Moch. Fiqih Prawira Adjie, The Jakarta Post, [Jokowi ‘violates the law’ for banning internet in Papua, court declares](#), 2020.

²⁴ KeepInOn Coalition, [2019 Report](#), 2020.

²⁵ HRW, [India Internet Clampdown Will Not Stop Misinformation](#), 2019

²⁶ Telenor group, [Directive to block social media service](#), 2021.

²⁷ Telenor group, [Myanmar authorities orders nationwide shutdown of the data network](#), 2021.

²⁸ Access Now, [Update: internet access, censorship, and the Myanmar coup](#), 15 February 2021.

After a series of bomb attacks that killed over 300 people in Sri Lanka in 2019, the government blocked major social media platforms, including Facebook and Twitter to prevent the circulation of disinformation online in the aftermath of the bombing. At first, some media cited Sri Lanka as an example where a shutdown countered the spread of dangerous “fake news”. However further reports²⁹ clarified how important social media access was to people’s safety and security following the attack.³⁰ **Especially during times of national emergency, access to accurate information is crucial.** Official information about the attacks provided by the government at that time was not adequate and traditional media outlets have been censored by public authorities.³¹

Recommendations

We therefore request that the Special Rapporteur make the following observations and recommendations for your report on disinformation to be presented at the 47th session of the Human Rights Council:

1. Call on states to stop internet shutdowns and provide effective remedies to those already affected.
2. Call on states to repeal laws criminalizing “fake news” and other repressive legislation that violates the rights to free expression and access to information.
3. Call on states to proactively share accurate and timely information in transparent and accessible formats about COVID-19, the measures taken to address the public health crisis and other important issues of public concern.³²
4. Call on states to recognise that regulating amplification of potentially harmful content, including disinformation, does have far reaching consequences on the right to freedom of expression and information.
5. Call on states to focus their legislative efforts on regulating the processes that online platforms deploy to govern content rather than users’ conduct or particular categories of user-generated content.
6. Call on the private sector to challenge censorship and service limitation requests from states, using all available tools of law and policy, in procedure and practice. Notify affected users and the public of any such requests and any orders implemented, early and often. Call on the private sector to adopt evidence and research-based responses to stop and prevent amplification of disinformation online.
7. Take active steps to further research and meaningfully understand the disproportionate impact of disinformation targeted at vulnerable groups while acknowledging the specific targetting of and impact on the situations of transgender people, those with non-binary

²⁹ Wired, [Don’t Praise the Sri Lankan Government for Blocking Facebook](#), 23 April 2019.

³⁰ Slate, [The Social Media Block Isn’t Helping Sri Lanka](#), 25 April 2019

³¹ Reporters without Borders, [2020 World Press Freedom Index](#), 2020.

³² For more recommendations for protecting freedom of expression and opinion and the right to impart and receive information to enable governments to fight the COVID-19 health crisis in a rights-respecting manner, please consult Access Now, [Fighting misinformation and defending free expression during COVID-19: recommendations for states](#), 2020.

gender identities, and gender non-conforming people, in addition to individuals' various intersecting identities including, but not limited to, race, ethnicity, sexual orientation, disability, class, language, religion, age, citizenship, and family status.



Access Now (<https://www.accessnow.org>) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

For more information, please contact: un@accessnow.org