FREEDOM OF EXPRESSION AND THE TELECOMMUNICATIONS AND INTERNET ACCESS SECTOR

Submission of ARTICLE 19: Global Campaign for Free Expression

2016

Introduction

ARTICLE 19 welcomes the decision of the UN Special Rapporteur on freedom of expression and opinion (Special Rapporteur) to engage in an in-depth study of the impact of the telecommunications and Internet access sector on freedom of expression. We believe that the telecommunications and Internet access sector have been critical in enabling access to and the dissemination of information. But we are also aware of a broad range of human rights concerns in this respect: in particular, this sector's impact on exercising the rights to freedom of expression and privacy. These concerns include the surveillance and disclosure of communications data and legislation, and the various measures taken to block services or impose restrictions outside of the rule of law. We expect that these concerns are likely to be ameliorated in the future through the rapid deployment of what has come to be known as the "Internet of Things,"[1] the increased usage of everyday objects connected to the Internet, and the power of both state and corporate surveillance. Hence, the Special Rapporteur's scrutiny of state regulation and the practices of sector actors is extremely important and timely.

ARTICLE 19 appreciates the opportunity to contribute to this study. We have previously contributed to the UN Special Rapporteur's work in this area,[2] namely his 2016 report on Freedom of Expression and the private sector in the digital age. This report set the scene for the in-depth study currently being conducted by the Special Rapporteur. This submission builds on our previous contribution and focuses on identifying:

I. Trends in state regulation of the telecommunications and Internet access sector;

II. The role of telecommunications companies (telcos) and the Internet access sector (including Internet exchange points, content distribution networks, and submarine cable consortia); and

III. The role of international Internet technical standards-setting bodies and Internet governance bodies in protecting and promoting freedom of expression, such as W3C, IETF, IEEE, ICANN, 3GPP, ISO, ITU-T, ITU-D, and ITU-R.

I. Trends in state regulation of the telecommunications and internet access sector

ARTICLE 19 finds that a vast range of laws and practices regulating the activities of telcos and Internet network services restrict the right to freedom of expression that the users of these services hold.[3] This restriction manifests from telecommunications laws, cybercrime laws, general laws criminalising certain types of content, laws on mass media, e-commerce laws, and others. The following include some of the key types of restrictions that are of concern.

Network shutdowns

Legislation in several countries enables governments to seize control of telcos for purported reasons of national security or emergency. The number of Internet shutdowns has been on the rise through 2016. For example:

- In Bahrain,[4] there have been reports from the village of Duraz over this past year of the deactivation of mobile Internet services by Bahrain's only mobile network providers, Batelco, VIVA, and Zain, and of unusable Batelco fixed-line DSL services. According to the reports, tests show that between 7PM and 1AM certain 3G and 4G cell towers belonging to Batelco and Zain appear to be turned off, and 2G cell towers broadcast notifications to phones indicating that mobile data services are not supported; furthermore, a device was detected on Batelco's Internet backbone that disrupted certain Internet traffic to and from Duraz between 7pm and 1am, while leaving other traffic undisrupted. From these findings, the report concluded that Batelco and Zain were likely deliberately disrupting both fixed-line and mobile data services in Duraz - possibly in accordance with a service restriction order from the Bahraini government, though this was unclear.

- In Bangladesh, the Telecom Regulatory Commission passed a decision in August 2016 to hold a telecommunications blackout, including mobile phone networks, in order to "assess the technical capability during an emergency."[5] All ISPs were notified of the Commission's decision and were asked to reply immediately upon receipt of the instruction to ensure a total Internet blackout of the particular area as instructed in the mail. The ISPs had to then confirm, through a reply to the Commission, that the blackout had been completed. The Commission's decision was taken during a meeting with the Association of Mobile Telecom Operators of Bangladesh.

Laws and practices enabling the blocking of access

In a number of countries, specific provisions grant powers, usually to a public body, to order the blocking of access to certain types of content, which are more or less broadly defined. For example:

- Under section 34 of Pakistan's Prevention of Electronic Crimes Act 2016, the Pakistan Telecommunications Authority has the power to order the removal or blocking of content "if it considers it necessary in the interest of the glory of Islam or the integrity security and defence of Pakistan or any part thereof, public order, decency or morality or in relation to contempt of court or commission or incitement to an offence under this Act;"[6]

- In Russia, between 2012 and 2013, the government passed several laws granting website blocking powers to several agencies including: the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor); the Prosecutor General's Office; the Federal Service for Surveillance on Consumer Rights and Human Wellbeing (Rospotrebnadzor); and the Federal Drug Control Service.[7] These blocking powers concern information ranging from extremist material to information about suicide, drugs, child pornography, materials that violate copyright, and calls for unsanctioned public actions or rallies. Any other information may be blocked by a court decision, provided that the court finds the content illegal.[8]

- In Turkey, Law No. 5651 concerning the regulation of publications on the Internet and the suppression of crimes committed by means of such publication provides extensive powers to block access to information, ranging from sexual exploitation of children to encouragement to commit suicide, obscenity, prostitution, and gambling, among others.[9] Under Article 8 of the law, both the courts and the Telecommunications and

Communications Presidency (TIB) can issue blocking orders. ISPs are required to block access to content within four hours of receiving notice of the order.[10]

- In France, a special police unit can order the blocking of child pornography and offences of incitement to terrorism or of publicly condoning terrorism.[11]

In some countries, blocking obligations are included directly in licensing obligations. Under the terms of the licence, operators may be required to block or filter certain types of content, such as pornography or content otherwise contrary to "good morals."

- In India, for instance, section 38 of the Telecommunications Unified Licence provides that "carriage of objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright and intellectual property Right etc., in any form, in the network is not permitted as per established laws of the country. Once specific instances of such infringement are reported to the Licensee by the enforcement agencies/Licensor, the Licensee shall take necessary measures to prevent carriage of Such Messages in its network immediately."[12] Operators' licences may be suspended or revoked if they fail to comply with the terms of their licence or other similar requirements;

- In Indonesia, operators may see their licence revoked if they engage in activities that violate the public interest, morals, security or public order;[13]

- In Bangladesh, licences are awarded by the Bangladesh Telecommunications Regulatory Commission in terms of the Bangladesh Telecommunication Act, 2001.[14] In terms of section 69 thereof, it is an offence for a person to offer another person engaged in the operation of a telecommunication apparatus "*to send an obscene, threatening or grossly insulting message*", and a separate offence if the latter person causes the message to be sent; the penalty for this is imprisonment not exceeding six months, or a fine not exceeding 50 thousand taka, or both.

In a number of countries, certain types of content, particularly child abuse images, are blocked by ISPs on the basis of self-regulatory arrangements or on the basis of public-private partnerships. ARTICLE 19 finds that self-regulatory measures pose a particular challenge from a human rights perspective. In particular, restrictions imposed by ISPs by virtue of cooperation agreements are typically not provided by law and cannot be challenged before the courts. At the same time, putting a framework in place for blocking certain types of content serves to further entrench censorship. Moreover, the content that may be blocked under the law is usually defined in overly broad terms.

Generally speaking, democratic countries tend to favour broad immunity from liability for ISPs by relying on public-private partnerships or the self-regulation of telecommunications companies, with a view to restrict particular types content such as child abuse images (e.g. the UK, see above). These countries also tend to rely on general content provisions in the law as a basis for blocking orders imposed by the courts.

- In the UK, for instance, the Internet Watch Foundation (IWF) - a registered charity funded by the European Union and the wider Internet industry - seeks to remove child abuse images from the Internet.[15] The IWF operates on the basis of a memorandum of understanding with the Association of Chief Police Officers and the Crown Prosecution Service. It provides the Internet Service Providers Association (ISPA) with a list of URLs that ISPA members are then required to filter by virtue of their ISPA membership: ISPA members are bound by ISPA's Code of Practice, which states that membership of the IWF is not mandatory but that ISPA cooperates with the IWF and that its procedures in this regard are mandatory for ISPA members.[16]

- Similarly, in Switzerland, blocking measures for certain types of content are only implemented following a dialogue between the competent authorities and ISPs.[17]

Other countries tend to adopt more specific laws that seek to restrict access to certain types of content online and provide for blocking powers by the courts or public authorities (e.g. Turkey, Russia, and France). While these laws provide a legal basis for restrictions on access to content (unlike self-regulatory measures), they also entrench censorship online. Nonetheless, Freedom House noted in its 2015 *Freedom on the Net* report that countries are increasingly moving away from website blocking and filtering towards content takedowns and other, more subtle, forms of censorship.[18]

Blocking of certain services or making these services illegal

A number of countries either block various instant messaging and Voice over Internet Protocol (VoIP) services or make such services illegal. For example:

- In Morocco[19], Skype, Viber, Tango, WhatsApp, and Facebook Messenger are among the applications whose VoIP calls have been blocked by telecom operators on 3G and 4G connections in January 2016 and ADSL connections in February 2016. According to Morocco Telecommunications Regulatory National Agency (ANRT), this was done on the basis that the providing VoIP services lacked the required licenses in the country. The ANRT ban was followed by the Governmental Decree of 2 June, which officially prohibited the use of VoIP services allegedly on competition grounds; the ban was only reversed in November 2016:[20]

- In China, any VoIP services that are not offered by state telcos are prohibited;

- In 2016, the United Arab Emirates President issued a number of special federal laws relating to Internet crimes, including a regulation that forbids anyone in the UAE from making use of virtual private networks (VPN). Under this law, anyone who uses a VPN or proxy server can be imprisoned and fined between Dh500,000 and Dh2,000,000 (approximately $136,000-$545,000) if they are found to use VPNs "fraudulently;"

- Other countries also attempted to impose similar bans on a limited basis. For example, in October 2013, Pakistan[21] proposed a three-month blanket ban on instant messaging and VoIP services in Sindh Province, allegedly on the grounds of national security. In 2012, the government of India ordered ISPs to intercept and identify the end users on unregistered VoIP calls in the states of Jammu and Kashmir.[22] In July 2016, access to WhatsApp was blocked on the basis of a court order on the grounds that WhatsApp has not shared information relating to criminal investigations with authorities; the block lasted for several hours.[23]

Other forms of restrictions

ARTICLE 19 also wishes to highlight the following restrictions that strengthen the surveillance capabilities of respective governments and facilitate the collection of information that can potentially be abused by authorities and become a tool of repression. All of these restrictions have a severe impact on the rights to freedom of expression and privacy, as well as the rights to freedom of association and assembly:

- Centralising SSL authority: For example, in December 2015, it was announced that the Kazakhstan Internet regulator - the Committee for Communications, Informatisation, and Information at the Ministry of Investment and Development - would be introducing a

national security certificate that Internet users would be required to install on their devices, including mobile phones;[24]

- Real name registrations: For example, in March 2016, the Chinese Ministry of Industry and Information Technology published a draft of its new Internet Domain Name Management Rules, which mandate that all Internet domain names in China must be registered through government-licensed service providers that have established a domestic presence in the country. This regulation would impose stringent regulations on the provision of domain name services. Under the rules, registrars issuing domain names must set up a management system from within Chinese borders and collect the personal information of domain name registrants. This means that all Chinese citizens will have to register their domain names inside China, with a real name verification model.[25]

- Data localization requirements: Regulations requiring companies to store and process data on servers physically located within national borders have been adopted in several countries. Governments often argue that these requirements are introduced to ensure the data's safety and to boost the local economy; however, they also enable state control over residents' online activities. For example:
  - In Russia, recently enacted legislation[26] requires "personal data operators" to "collect, store, and process any data about Russian users in databases inside the country and to inform Russian authorities of the location of their data centres;" and also provides authorities easier access to information and imposes harsh penalties on non-compliant companies. The law also restricts Russian users' access to any website that violates the nation's data protection laws;
  - In Vietnam, a 2013 law includes an explicit requirement to store data on servers within the country.[27]

Intermediary liability

Again, the rules governing liability are usually scattered across several areas of the law, from e-commerce laws[28] to cybercrime laws,[29] and even to the general laws of civil and criminal liability.[30] Regardless of where these provisions may be found, ISP-liability regimes can be divided generally into two main types:

- Laws granting broad immunity: This is the case, for instance, in Brazil[31] and in the US.[32] In the EU, ISPs are granted broad immunity from liability as mere conduits, although Article 12(3) of the E-Commerce Directive provides that this is without prejudice to the possibility of a court or administrative authority, in accordance with Member States' legal systems, requiring the ISP to terminate or prevent an infringement;[33] or

- Laws imposing criminal liability for the dissemination of a variety of content: In Bangladesh, for example, sections 57 and 59 of the ICT Act 2006 establish that it is an offence for any person to deliberately publish or transmit, or cause the publication or transmission of any material that is deemed to be fake, obscene, prejudicial to the image of the State, or hurtful to religious beliefs, on a website or in any electronic form.[34] Similarly, in Indonesia, Article 27(1) of the Electronic Information Transactions Law prohibits distributing, transmitting, or facilitating the accessibility of contents "against propriety."[35] It is not always clear, however, whether these broad provisions are used against ISPs or whether the equivalent provisions of the Telecommunications Law are used.[36] In Thailand, section 20 of the Computer Crimes Law B.E. 2550 (2007) provides that where information is deemed to negatively affect national security (including *lèse majesté*) or to potentially violate public order or good morals (such as pornography), the authorised officials may, with the approval of the Minister of the MICT, petition the

relevant court with jurisdiction to halt the dissemination of information directly, or to order a service provider to do so.[37]

Laws of general application
In some countries, ISPs may be ordered by the courts to block access to content deemed unlawful under laws of general application. For example:

- In the United Kingdom, for instance, the courts' power to order the blocking of websites that infringe on copyright derives both from the Copyright, Designs and Patents Act 1988 and the general power of the courts to issue injunctions. Failure to comply with a court order constitutes an offence of contempt of court.[38]

- The same approach is generally followed in Germany[39] and in the Netherlands.[40]

National security and emergency powers
In several countries, telecommunications laws provide for broad powers in case of an emergency. These laws can be used by governments to justify Internet shutdowns. For instance:

- In Egypt, Article 67 of the Telecommunications Law grants "competent authorities" the power to seize control of any telecommunication service of any operator or provider in the case of natural or environmental disaster, or during "declared periods of general mobilization" or "any other case concerning national security". The government relied on this provision to justify cutting off access to all communications services in January 2011.[41]

- The Telecommunications Industry Dialogue provides detailed information about similar emergency provisions in a number of countries on its platform.[42]

II. The role of telecos and the Internet access sector

As outlined above, States around the world have enacted a range of laws that negatively affect individuals' rights in relation to digital technologies. Consequently, telcos and the Internet access sector may infringe on the rights of users by complying with requests or requirements imposed on them by States under these laws.

At the same time, telcos and the Internet access sector may violate the rights of users through actions taken of their own volition for business or commercial reasons.[43] This section focuses on such practices. While there are various instances of telecos and the Internet access sector complying with the demands of States in a manner that facilitates negative impacts on human rights, there is a growing trend among these actors towards ascertaining ways through which this harm may be mitigated; some such efforts are also highlights here.

In our earlier submission to the Special Rapporteur, ARTICLE 19 outlined various efforts undertaken on the international plane in an attempt to more readily secure an adherence to human rights standards by private actors. This has included, in particular, the UN Guiding Principles on Business and Human Rights (Ruggie Principles) and National Action Plans that some States have developed. ARTICLE 19 believes that the Special Rapporteur should reiterate that telcos and the Internet access sector should abide by the Ruggie Principles, set in place human rights policies, and conduct due diligence assessments of the impacts of all their operations on human rights. Such assessments should identify both the actual and

potential impacts, and these actors should subsequently act on these assessments, monitor and track their performance in this regard, and provide remedies in cases of violations. Moreover, these actors should adjust their responses to changing risks and communicate such matters to the public.

In our submission to the 2016 report of the Special Rapporteur, ARTICLE 19 outlined a number of human rights concerns related to private actors, including telcos and the Internet access sector (in particular surveillance). In this respect, we also suggest that the Special Rapporteur explore the addtional following issues.

Terms of service

It is common practice for companies to have terms of service that contractually regulate their relationships with users, and that users are required to abide by in order to make use of the services. When considering terms of service, first and foremost, it should be determined whether the terms of service are adequately clear and precise so that users can properly understand the impact of consenting to the terms of service, and are able to amend their behaviour accordingly if necessary. In terms of restrictions on the right to freedom of expression, ARTICLE 19 believes that terms of service should also comply with the general principles of the three-part test of legality, proportionality, and necessity contained in Article 19(3) of the International Covenant on Civil and Political Rights.

It must also be determined whether users have alternatives if they choose not to consent to the terms of service in question; whether the restrictions contained in the terms of service serve a wider public policy objective; and the nature of the restrictions that are enacted by the terms of service. Although telcos and ISPs may seek to argue that as private entities, they are at liberty to determine their own engagements with their users in line with what is best suited to their business, this view cannot be countenanced - particularly in circumstances in which a particular company is so dominant in the market that users are effectively left with no meaningful alternative to abiding by its terms of service. In such circumstances, it is all the more incumbent upon relevant telcos and ISPs to ensure that they comply with human rights standards.

There is typically little redress for users whose rights of freedom of expression are negatively impacted by the terms of service of telcos and ISPs. Furthermore, there are inadequate measures in place to ensure accountability for decisions taken in accordance with the terms of service. This is exacerbated by the fact that little information is known about how often action is taken by telcos and ISPs to enforce the terms of service, as this data does not generally form part of transparency reporting processes.

Access to the Internet

ARTICLE 19 suggests that the Special Rapporteur should examine the following issues related to telcos/the Internet access sector and the access to the Internet:

- Net neutrality and content agnosticism: ARTICLE 19 believes that in this report, the Special Rapporteur should reiterate the importance of net neutrality and content agnosticism. The principle of net neutrality states that network traffic should be treated identically regardless of payload, with some exception for cases in which prioritization is necessary for the effective governance of traffic flows - for instance, when there may be the threat of delays of sensitive packets, based on the header. Content agnosticism prevents payload-based discrimination against packets. This is important because changes to this principle can lead to a two-tiered Internet, where certain packets are

prioritized over others on the basis of their content. Effectively, this would mean that although all users are entitled to receive their packets at a certain speed, some users become more equal than others.

- Public Wi-Fi "hot spots": Public WiFi hotspots are such areas where anyone with a digital device can connect to the Internet are either the result of private initiatives (intended to attract individuals to certain commercial establishments – e.g. coffee shops or fast food chains) or are provided by governments or municipalities over vast public spaces. Various local and municipal authorities are now developing free Wi-Fi networks at a rapid pace, both on their own and in collaboration with private operators. The conditions for services take various forms: for example, private companies may offer such services in exchange for their governmental telecommunications contracts, for displaying their advertising, or for providing services on publically owned networks. As with the previous issue, users must accede to the networks' terms of service, which are often formulated in such a way as to significantly undermine the contractual position of users. Moreover, users are often unaware that these networks also facilitate official and unofficial surveillance - using a public Wi-Fi networks makes them vulnerable by rendering their data and communication unprotected.

- Efforts to limit the Internet access: In some countries, telcos have prevented the efforts of local governments to provide Internet access. For example, in the US state of North Carolina, ISPs successfully lobbied for a bill that prohibits municipal governments from providing Internet access to its residents, even when that access is better or cheaper than the private sector alternative.[44]

- Last mile connectivity: "Last mile technology" is a term used within the telecommunication industry to describe the final leg of connectivity used to link the end customer to a telecommunication network. These technologies includes LAN (Local Area Network), wireless network, DSL (Digital Subscriber Line), CATV (cable), fibre optics, satellite technology, FSO (Free-space optical communication), radio waves, POTs (Plain Old Telephone System and ISDN (Integrated Services Digital Network). Compared to general Internet infrastructure, last mile ISPs are, in many places, monopolies (or oligopolies) "where the lack of competition and broadband providers' physical control of the communications conduit create a clear bottleneck"[45] in the distributed nature of the Internet.

- Open/unlicensed spectrum: One of the main barriers to accessing the Internet is the availability of affordable spectrum. This issue can be resolved if governments release sufficient spectrum at affordable cost and adopt a flexible framework for regulating both licensed and unlicensed spectrum. Unlicensed spectrum allows the public to freely access services without a license. As a result, anyone is free to access these unlicensed bands to operate devices. This open scheme allows devices to connect through technologies like Wi-Fi, keeping prices low for consumers and giving innovators the spectrum they need to develop new products. The Special Rapporteur should provide recommendations to States and companies on facilitating open spectrum and adopting a comprehensive open spectrum agenda.

- Infrastructure sharing: Another solution of removing barriers to accessing the Internet is voluntary infrastructure sharing. Research shows the important role that infrastructure sharing plays in reducing costs and improving coverage for broadband. For example, research conducted by APC shows that the cost of network deployment can be reduced dramatically if operators collaborate with each other in deploying shared fibre optic backbones, or masts, for wireless broadband. The report also shows that even greater

impacts have been noted when other utility infrastructures such as roads, rail lines, and power cables are shared with telecom operators.[46]

Hence, the report is an opportunity for the Special Rapporteur to encourage States to introduce measures for adopting effective infrastructure sharing guidelines and regulations. Further, efficient network interconnection and traffic exchange are essential to improving access to and the affordability of the Internet. The Special Rapporteur should highlight that IXPs should not be captured by any one interest, whether by governments or private companies, to further their own benefit at the expense of others. They should be neutrally operated and governed by shared agreements among the relevant stakeholders.

- 5G technologies and respect for human rights: ARTICLE 19 suggests that the Special Rapporteur closely monitor the developments surrounding 5G, and advocates for telcos to deploy and develop it in full respect of human rights. 5G is the next generation of mobile internet connection (tentatively scheduled for rollout in 2020), which will enable faster Internet connections and more portability. It is seen not merely as an evolution of mobile networks, but as a new technology that will allow for entirely new capabilities in a number of fields: it will impact Internet speed, bandwidth, power consumption for devices, and human rights. It promises a major shift in the way radio spectrum is allocated and used, allowing for a hugely expanded "Internet of Things," as well as a dramatic improvement in the speed of content. At the same time, it is unclear what standards and protocols this new connectivity will use, how much it will cost, or what infrastructure will be needed to implement it. How these decisions are made will drive the impact of 5G on human rights - in particular, the right to freedom of expression and access to information. 5G could even replace wired Internet, at least in urban centres: this would give even more power to telcos, centralising power to one stakeholder group and potentially creating a chokehold of control over the Internet. 5G also poses major risks to human rights. The principle of net neutrality may prove to be genuinely threatened by 5G, as the diversity of needs to be met by 5G networks may create the space for an argument in favour of developing 'fast lanes' for certain types of content and special treatment of some data packets, or even 'bandwidth throttling'. This violation of net neutrality poses more of a danger than just fast streams and special treatment. It might result in the fragmentation of the Internet itself: risking the loss of the benefits of the network in terms of freedom of expression and freedom to receive information.

  In July 2016, some of the world's largest telecoms companies, including BT, Nokia, Orange, and Vodafone, signed a "5G Manifesto,"[47] aiming to drive forward the development of the next-generation network. This manifesto has been strongly criticised,[48] as it calls into question the necessity of current net neutrality standards in Europe. The companies claim that the guidelines may limit innovation, warning that the current European net neutrality guidelines "create significant uncertainties around 5G's potential for return on investment." ARTICLE 19 suggests that the Special Rapporteur highlight the need for respecting human rights in all 5G discussions, and supports the creation of a coordinated and inclusive action plan on standards, spectrum, and infrastructure development in the deployment of 5G technologies.

Transparency and accountability

Various initiatives at different levels currently exist to promote transparency and the respect for human rights, including those led by companies, by governments, and by civil society, as well as multi-stakeholder initiatives. With particular regard to freedom of expression and privacy in the ICT sector, including telecos and ISPs, this includes:[49]

- Company-led initiatives, such as the Telecommunications Industry Dialogue[50] and GSMA Mobile Privacy Initiative;[51]

- Multi-stakeholder initiatives, such as the Global Network Initiative.[52] the Global Network Initiative encourages both network operators and governments to consider the following areas of disclosure:[53]
    - The country's laws that apply to the blocking and interception of communication traffic, covering both targeted and mass interventions; and, in the case of companies, how they interpret the law;
    - Whether operating licences are publicly available, and if so, where they are located;
    - The number of government requests for communications metadata;
    - Whether government agencies have direct access to communications metadata retained by telecommunications companies through electronic means or through physical open access to company facilities;
    - The number of government requests to intercept communications content under a legal interception arrangement;
    - Whether parallel traffic feeds exist from the telecommunication network to one or more government agencies, effectively granting the government unlimited access to monitor either intra-country communications or inter-country communications;
    - The number of government requests to block access to websites with a top-level breakdown of the reasons;
    - The number of government requests to close down any part of the in-country network with details of the incidents;
    - Government requests to transmit specific messages to the users of network services without disclosing that these messages are from the government.

- Civil society initiatives, such as Ranking Digital Rights,[54] IHRB Digital Dangers[55] and European Digital Rights.[56] The EFF has also launched the "Who has Your Back" initiative, which ranks online service providers based on their practices of handling government requests;[57] in terms of this work, the EFF uses five criteria to assess company policies and practices:[58]
    - Industry-accepted best practices, including whether the company publishes a transparency report and whether it publishes a law enforcement guide explaining how it responds to demands from government;
    - Whether the company tells users about data requests from the government;
    - Whether the company publicly discloses its data retention policies;
    - Whether the company discloses the number of times governments seek removal of user content or accounts, and how many times the government complies;
    - Whether the company has pro-user public policies: in particular, regarding opposition to backdoors.

ARTICLE 19 believes that the Special Rapporteur's report should reiterate the importance of transparency reporting by telecommunication and Internet access sector actors, including a focus on the protection of the right to freedom of expression, as a crucial contribution to greater accountability and respect for human rights. We believe that transparency reports should contain the types of information listed in the Ranking Digital Rights ('RDR') indicators for freedom of expression.[59]

III. The role of the technical standard setting bodies and the Internet governance bodies

Internet technical standards-setting bodies and Internet governance bodies develop and promote voluntary standards and protocols for telecommunications, Internet access, and the

World Wide Web, respectively, and may have implications for the exercise of freedom of expression. Hence, ARTICLE 19 suggests that the Special Rapporteur highlights the need of these bodies to respect the human rights standards and in their operations. In particular, we recommend he focuses on the following bodies:

- The International Telecommunication Union – ITU. ITU comprises three sectors, each managing different aspects of telecommunications (Radiocommunication - ITU-R,[60] Standardization - ITU-T,[61] and Development - ITU-D[62]). The ITU has traditionally operated under a very exclusive, top-down decision making process. As a result, its processes lack the transparency, openness, and inclusiveness for all relevant stakeholders - in particular, civil society.

- The Internet Corporation for Assigned Names and Numbers – ICANN. ICANN was created in 1998 as a non-profit public benefit corporation under Californian law and under the mandate of the US government. ICANN's primary role has been to take responsibility for the technical management of Internet domain names and addresses: developing policies governing the introduction of new generic Top Level Domains (gTLDs) into the Domain Name System (DNS), coordinating the assignment of technical Internet protocol parameters, and allocating Internet numbering resources (IANA). ICANN is a hybrid organisation as both a global corporate operation as well as a global governance body, responsible for particular Internet functions through the development of Internet policy. These policies and the conduct and decisions of registries and registrars can profoundly affect multiple stakeholder groups, including individuals, businesses, organisations, and governments. Policy development takes place through a unique multi-stakeholder, bottom-up decision making model, setting ICANN apart from typical business enterprises. ICANN's IANA transition in September 2016 has prompted discussion on furthering its accountability and transparency. Global debates exploded following the first application round of the new gTLDs in 2012, set against the backdrop of the creation of the UNGPs in 2011. There is a vibrant and diverse discourse within the ICANN community about the overall remit, values, principles, and practices of ICANN itself. Emerging from this discourse is the question of the relationship between ICANN activities and human rights.

  Under Article 4 of ICANN's Articles of Incorporation, ICANN is committed to "carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law." Whether the "relevant principles of international law and applicable international conventions" include international human rights instruments has yet to be explicitly stated. In the process leading to the IANA transition a new Core Value was added to the ICANN bylaws which states that: '*within the scope of its Mission and other Core Values, [ICANN will] respect[ing] internationally recognized human rights as required by applicable law.*' As well as an addition that says that this bylaw will not come into effect until a Framework of Interpretation is developed. This seems like a good step, for which ICANN and its community should be commended. It is however still to be seen how this framework will be implemented. On this there are parallel, on-going discussions regarding the best way to develop and implement policies relating to ICANN and human rights. To assist this process, a Cross Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights (CCWP-HR) was established in 2015 with this particular focus. Another stream of inquiry focuses on ICANN's overall corporate social responsibility (CSR), its scope, and the necessary actions stemming from this responsibility, such as CSR and transparency reporting as well as Human Rights Impact Assessments becoming an inherent part of the Policy Development Processes as well as of ICANNs operations.

- The Internet Engineering Task Force – IETF. IETF is one of the most important players in standardizing the technical architecture of the Internet. It plays a crucial role in managing the logical layer of the Internet, and in designing the standards and protocols that define how information flows across the network. The IETF essentially creates voluntary standards that maintain the interoperability and usability of the Internet. It has no official membership. Its work is mostly done over the publicly available email lists and during three annual meetings. Decisions at the meetings are made on the basis of achieving a 'rough consensus,' expressed by 'humming'.

  The Human Rights Protocol Considerations Research Group ("HRPC") of the Internet Research Taskforce, IRTF (a sister organization of the IETF) is chartered to research how standards and protocols (the rules by which the internet functions) can enable, strengthen, or threaten human rights. It is tasked with exposing the relationship between protocols and human rights - with a particular focus on the rights to freedom of expression and freedom of assembly – in order to propose guidelines that would protect the Internet as a human rights-enabling environment in future protocol development. This process takes a similar approach to the work done for Privacy Considerations in RFC 6973, and serves to increase the awareness in both the human rights community and the technical community on the importance of the impacts of the technical workings of the Internet on human rights. The work on this document[63] by the HRPC is nearing completion, after which the recommendation could be brought into the IETF to see how Human Rights Protocol Considerations could become inherent part of the standards developing process, which would be a technical translation of Human Rights Impact Assessments as outlines by the UN Guiding Principles for Business and Human Rights.

- The World Wide Web Consortium - W3C. W3C is an international community that develops open standards[64] to ensure the long-term growth of the Web. W3C operates under the Code of Ethics and Professional Conduct[65] furthermore the W3C has done extensive work on accessibility standards which have improved access to the Internet for people with different physical limitations. Finally W3C is currently also working on a standard to implement DRM which has a huge potential impact on freedom of expression on the Internet as well as on the sovereignty of Internet users.[66]

- The 3rd Generation Partnership Project - 3GPP. 3GPP unites telecommunications standards development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as Organizational Partners, and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, and quality of service - and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks. We also point out 3GPP is an only standard setting body (not multi-stakeholder mechanism) developing 5G. ARTICLE 19 reiterates that in this report, the Special Rapporteur can issue strong recommendations that the 5G-development process incorporates human rights, and that this development is done through stakeholder participation and transparency.

- The Institute of Electrical and Electronics Engineers, Incorporated – IEEE. IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity, with over 400,000 members in more than 160 countries. In April 2016, in order to address the ethical dimensions of their work the IEEE launched the Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems[67]. The initiative aims to identify needs and build consensus for standards,

certifications, and codes of conduct regarding the ethical implementation of intelligent technologies. It aims to achieve three specific goals: draft a document discussing how Artificial Intelligence and Autonomous Systems (AI/AS) intersect with ethical concerns, educate technologists about the societal impact of the technology they build, and make recommendations for the development of technical standards based on the ethical concerns identified. On 13 December 2016, the Global Initiative launched its first document, *Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems*,[68] based on a series of meetings, and the work done by the various working groups (currently being subject of consultation and final version will be released in 2017). Here, the Special Rapporteur can recommend that this process continues to ensure that strong ethical frameworks are paired with strong legal frameworks, based on international human rights standards.

Telcos, the Internet access sector, and technical standards bodies are respective points for centralization or convergence and coordination in a distributed Internet infrastructure. At the same time, the points of centralization or convergence in a distributed infrastructure are, by definition, potential points for control.

The relationship between human rights and standards-setting bodies, particularly in relation to Internet protocols and architecture, is a new research challenge that requires the development of a consistent methodology and bringing together human rights experts and the community of researchers and developers of Internet standards and technologies. The Special Rapporteur can contribute to this process. He should also highlight that a proper assessment of this relationship can only be conducted through transparent operations and procedures.

Recommendations

In light of the above, ARTICLE 19 suggests that the Special Rapporteur make the following recommendations in his 2017 report:

- States should review all legislation relevant to the telecommunications and Internet access sector – in particular, those highlighted in Section I of this submission - and bring it to full compliance with international human rights standards, and specifically with those on the right to freedom of expression;

- States must refrain from Internet shutdowns and other disruptions affecting the use of and access to communication tools. Internet governance bodies, together with the telecommunication industry, should continue to raise awareness about the negative impact of these shutdowns and increase accountability for the stability of networks;

- As for blocking and filtering, States should ensure that blanket filtering is explicitly prohibited by law. Filtering should be user-controlled and transparent. Although the use of filters and blocking measures should be rejected as a matter of principle, the blocking/filtering measures can be compatible with international human rights standards only under very rare circumstances. In particular, any requirement to block unlawful content must be provided by law, and should only be permitted in the respect of content that is unlawful or can otherwise be legitimately restricted under international standards on freedom of expression. Blocking should only be ordered by an independent and impartial court or adjudicatory body. Any order to block access to content should be limited in scope and strictly proportionate to the legitimate aim pursued. Moreover, in order for blocking orders to be maximally compatible with international human rights standards, the following procedural safeguards should be put in place:

- When a public authority or third party applies for a blocking order, ISPs or other relevant internet intermediaries must be given the opportunity to be heard in order to contest the application;
- There should similarly be procedures in place that allow other interested parties, such as free expression advocates or digital rights organisations, to intervene in proceedings in which a blocking order is sought;
- Users must also be given a right to challenge, after the fact, the decision of a court or public body to block access to content. Whenever certain content has been blocked by such an order, moreover, anyone attempting to access it must be able to see that it has been blocked and a summary of the reasons why it was blocked, in order that they may have the opportunity to challenge the decision. In particular, blocked pages should contain the following minimum information:
  - The party requesting the block;
  - The legal basis for the decision to block; the reasons for the decision in plain/user friendly language (not legal jargon), HTTP status code 451[69] should be served;
  - The case number, if any, together with a link to the relevant court order;
  - The period during which the order is valid;
  - contact details in case of an error;
  - Information about avenues of appeal or other redress mechanisms.
- ISPs should have a remedy to challenge blocking orders issued by the courts or administrative authorities. The ISPs should not be required to comply with blocking orders that have no basis in law, either because the content itself is lawful or because the authority purporting to order the blocking measures is acting *ultra vires* its powers.

- States, telcos, and the Internet access sector should respect the principles of net neutrality/content agnosticism;

- States, in cooperation with the industry, should adopt a broad range of measures to remove barriers to accessing the Internet, including but not limited to: access to open spectrum, infrastructure sharing, and other measures. They should also ensure that human rights are fully respected in all 5G discussions, action plans, standards-setting and infrastructure development in 5G technologies deployment;

- Telcos, the Internet access sector, and standards-setting bodies must engage in more proactive disclosures of information through transparency reports and the publication of the regulatory frameworks by which they operate;

- Telcos and the Internet access sector should
  - Complete human rights impact assessments for their services, policies, and infrastructure and involve independent external parties in these impact assessments;
  - Adopt clear Terms and Conditions (terms of service) that are understandable for the users;
  - Rigorously consider requests from states that may hamper users' rights of freedom of expression, and make all reasonable endeavours to mitigate restrictions to rights;
  - Develop individual or industry frameworks for standards;
  - Seek to establish remedies to enable users to challenge decisions that have been taken;

- Standards bodies should:
  - Stimulate galvanisation of the distributed nature of the Internet and end-to-end principles;

- Stimulate minimising the exposure of PI (data minimisation);
- Assert their responsibility as a point of coordination in a network that is fundamental for exercising human rights;
- Ensure that standards development and negotiations are transparent and open to all stakeholders and that standards are freely available to all;
- Allow for internationalization of protocols (global network, not only user facing);
- Ensure that standards undergo a human rights impact assessment to analyze their potential impact on human rights, once deployed. They should also facilitate and promote standardised human rights impact assessments for all telcos and standards bodies.

---

[1] The International Telecommunication Union defines the Internet of Things as "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies;" New ITU Standards Define the Internet of Things and Provide the Blueprints for Its Development, ITU.
[2] ARTICLE 19, Freedom of Expression and the private sector in the digital age, March 2016.
[3] For country information on the regulatory framework of telecommunications services, see the "resource" page of the Telecommunications Industry Dialogue.
[4] Bahrain Watch, Time for some Internet Problems in Duraz': Bahraini ISPs Impose Internet Curfew in Protest Village.
[5] Star Online, Drill on shutting down internet, mobile networks today, 1 August 2016.
[6] Pakistan, A Bill to Make Provisions for Preventions of Electronic Crimes..
[7] See Freedom House, *Freedom on the Net,* 2015, Russia country report, page 653.; see also ARTICLE 19, Digital Rights in Russia.
[8] *Ibid.*
[9] See Council of Europe Study on Filtering, Blocking and Takedown of Illegal Content, December 2015, Turkey country report.
[10] *Ibid,* Council of Europe Study.
[11] See Decret no. 2015-125 of 5 February 2015 concerning the blocking of websites inciting to or publicly condoning acts of terrorism or websites disseminating child abuse images; see also Council of Europe study, *op. cit.,* France Country Report; and ARTICLE 19, France: ARTICLE 19 challenges lawfulness of administrative blocking, 30 July 2015.
[12] India, Ministry of Communications and IT Department of Telecommunications, India License Agreement for Unified License.
[13] See Articles 21 and 45 of Indonesia Telecommunications Law, no 36 of 1999.
[14] ITU, Bangladesh profile (2015),.
[15] https://www.iwf.org.uk/about-iwf
[16] See COE Study, UK country report cited at fn 21.
[17] See COE Study, *op cit.,* Comparative Considerations.
[18] See Freedom House, *Freedom on the Net,* 2015 p.1.
[19] Middle East Eye, Morocco banned Skype, Viber, WhatsApp and Facebook Messenger, 9 March 2016.
[20] Telco TV News, Morocco decree makes ban on VOIP apps official, 14 June 2016; and Morocco World News, Morocco's VoIP Ban Quietly Reversed Without Official Announcement, 24 October 2016
[21] ARTICLE 19, ARTICLE 19 and Bytes for All condemn proposed ban on instant messaging, 9 October 2013.
[22] EFF, This Week in Internet Censorship: India, Iran, Brazil, Russia, 15 May 2012.
[23] ARTICLE 19, Brazil: WhatsApp services blocked nationwide in violation of freedom of expression, 22 July 2016.
[24] Bits, Corporate actors must not facilitate human rights violations through new Chinese rules, 3 December 2015.
[25] ARTCLE 19, Corporate actors must not facilitate human rights violations through new Chinese rules, 2 December 2016.
[26] The Federal Law 242-FZ, in effect from 1 September 2015.
[27] Albright Stonebridge Group, Data Localization: A Challenge to Global Commerce, September 2015.
[28] See the EU's E-Commerce Directive 2000 or Kenya's draft Information and Communications (Electronic Transactions) Regulations, 2016.
[29] See ARTICLE 19, Legal analysis of the Ethiopia Computer Crime Proclamation, 2016.
[30] See APC, *The liability of Internet intermediaries in Nigeria, Kenya, South Africa and Uganda: an uncertain terrain,* 2012: the report notes the lack of clear legal framework in Kenya and Nigeria. In Kenya, several draft pieces of legislation are currently being consulted on, including the draft regulations on electronic transactions cited at Footnote 11.
[31] See Article 18, the Marco Civil da Internet.

[32] Communications Decency Act 1996, 47 U.S.C. § 230(c)
[33] See Article 12 of the E-Commerce Directive 2000.
[34] See Telecommunications Industry Dialogue: Bangladesh,; for a more detailed legal analysis of the ICT Act 2006, see ARTICLE 19, Analysis of the Bangladesh ICT Law..
[35] See ARTICLE 19, *Navigating Indonesia's Information Highway*, March 2013.
[36] *Ibid.*
[37] See Telecommunications Industry Dialogue: Thailand.
[38] For more details, see COE study, *op.cit.;* or the UK country report.
[39] *Ibid.*, Germany country report.
[40] *Ibid.,* Netherlands country report.
[41] See ARTICLE 19 and AFTE, Egypt: Telecommunication Regulation Law, April 2015.
[42] https://www.telecomindustrydialogue.org/resources/country-legal-frameworks/
[43] See, for instance, Ranking Digital Rights,
[44] Ars technical, Cable-backed anti-muni broadband bill advances in North Carolina, 30 March 2011.
[45] Brief for Center for Democracy & Technology as Amicus Curiae Supporting Respondents, *Verizon v. FCC*, No. 11-1355 (D.C. Circ. Nov. 15, 2012)
[46] APC, Unlocking broadband for all: Broadband infrastructure sharing policies and strategies in emerging markets, 24 April 2015.
[47] 5G Manifesto for timely deployment of 5G in Europe, 7 July 2017.
[48] The Register, EU operators' 5G manifesto misses the point, 13 July 2016.
[49] Global e-Sustainability Initiative, Human rights and the ICT sector: A thought leadership agenda for action for GESI, p19,. Further information about these initiatives, including their members, aims and work undertaken, can be found at pp 20-23 thereof.
[50] See http://www.telecomindustrydialogue.org/.
[51] GSMA Mobile Privacy Initiative.
[52] See http://globalnetworkinitiative.org/.
[53] Global Network Initiative, Opening the lines: A call for transparency from governments and telecommunications companies, pp 21-22.
[54] See http://rankingdigitalrights.org/.
[55] See http://www.ihrb.org/about/programmes/digitaldangers.html.
[56] See http://edri.org.
[57] EFF, Who has your back?.
[58] *Ibid*, pp 5-7.
[59] The RDR indicators are available from here.
[60] The Radiocommunication Sector (ITU-R) is a sector within the ITU that manages global radio communication, satellite orbits and derived technologies and services, such as wireless communication, broadband Internet, meteorology, TV broadcasting, and cellular communication.
[61] Under the ITU, Telecommunication Standardization (ITU-T) coordinates with all entities involved with creating standards in the telecommunications industry.
[62] Under the ITU, Telecommunication Development Sector (ITU-D) organizes ICT/telecom events, seminars and workshops and works with the industry to develop telecom products and solutions.
[63] Research into Human Rights Protocol Considerations, draft-irtf-hrpc-research-07
[64] W3C, All Standards and Drafts.
[65] W3C, Code of Ethics and Professional Conduct.
[66] See, EFF, You Can't Destroy the Village to Save It: W3C vs DRM, Round Two, 12 January 2016; or Joi Ito, A recent discussion about DRM with Richard Stallman, Danny O'Brien and Harry Halpin, 6 April 2016. See also, W3C, Accessibility.
[67] 'IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems.
[68] Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems, 2016.
[69] In computer networking, HTTP 451 Unavailable For Legal Reasons is an error status code of the HTTP protocol to be displayed when the user requests a resource which cannot be served for legal reasons.