United Nations A/HRC/35/22

General Assembly

Distr.: General
30 March 2017

Original: English

Human Rights Council
Thirty-fifth session
6-23 June 2017
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

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

Note by the Secretariat

The Secretariat has the honour to transmit to the Human Rights Council the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, prepared pursuant to Council resolution 25/2. In his two previous reports to the Council, the Special Rapporteur focused on the freedom of opinion and expression in the digital age, detailing how encryption and anonymity tools provide the security necessary for the exercise of freedom of expression (A/HRC/29/32) and mapping the ways in which the information and communications technology sector implicates freedom of expression (A/HRC/32/38). In the present report, he addresses the roles played by private actors engaged in the provision of Internet and telecommunications access. He begins by examining State obligations to protect and promote freedom of expression online, then evaluates the digital access industry's roles, to conclude with a set of principles that could guide the private sector's steps to respect human rights.

GE.17-05047(E)
1705047

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

Contents

I. Introduction

1. States increasingly rely on the digital access industry to control, restrict or monitor expression online. When authorities seek to disconnect users from websites, social media, or the Internet entirely, they frequently require the assistance of Internet service providers (ISPs). They interfere with the Internet exchange points (IXPs) that facilitate traffic into or within a country. They access private communications and other personal data held by telecommunications providers. Today, many of these actors are privately owned or operated. Under protest, in silent acquiescence or as willing participants, they are often essential to State censorship and surveillance. What governments demand of private actors, and how those actors respond, can cripple the exchange of information; limit journalists' capacity to investigate securely; deter whistle-blowers and human rights defenders. Private actors may also restrict freedom of expression on their own initiative. They may assign priority to Internet content or applications in exchange for payment or other commercial benefits, altering how users engage with information online. Companies that offer filtering services may influence the scope of content accessible to their subscribers.

2. States and private actors both implicate the freedom of expression. State obligations to protect freedom of expression are clear, but what do private actors owe their users? How should they respect freedom of expression? What steps are they taking to assess and address the risks that their responses to government actions and policies might pose to freedom of expression and privacy? How much information should they share with their customers about State demands and requests? When they are directly involved or linked to abuse, what remedies should be available to individuals or the broader public whose interests are at risk?

3. The private actors that make digital access possible mediate and enable the exercise of freedom of expression. To be sure, States drive most censorship and surveillance. But just as States often, but not always, rely upon providers to take the actions that make censorship possible, we as users — beneficiaries of the remarkable advances of the digital age — deserve to understand how those actors interact with one another, how these interactions and their independent actions affect us and what responsibilities providers have to respect fundamental rights.

4. The present report is the result of over one year's worth of study and consultation that began with the mapping in 2016 of the information and communications technology (ICT) sector (see A/HRC/32/38).[1] In response to a call for submissions,[2] the Special Rapporteur received 25 submissions from States; 3 from companies; 22 from civil society, academics and others; and 1 confidential submission. In addition, the Special Rapporteur convened a brainstorming session hosted by ARTICLE 19, in London in July 2016, a meeting of experts at the Human Rights Institute, University of Connecticut, United States of America, in October 2016, a regional consultation with the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, in Guadalajara, Mexico, in December 2016, and a regional consultation in Beirut in February 2017.[3]

[1] I want to thank Amos Toh, legal adviser to the mandate and Ford Foundation Fellow at University of California, Irvine, School of Law, for his expert research and analysis as well as coordination of substantial and essential research conducted by law students in University of California, Irvine, International Justice Clinic.

[2] See https://freedex.org/new-call-for-submissions-freedom-of-expression-and-the-telecommunications-and-internet-access-sector/.

[3] Submissions may be found on the website of the mandate. An overview of the consultations held and input received in the preparation of the present report may be found in a supplementary annex also available from the website of the mandate.

II. State obligation to protect and promote freedom of expression online

5. International human rights law establishes the right of everyone to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers, and through any media of his or her choice (see Universal Declaration of Human Rights, art. 19; and International Covenant on Civil and Political Rights, art. 19). The Human Rights Council and General Assembly have reiterated that the freedom of expression and other rights apply online (see Council resolutions 26/13 and 32/13; General Assembly resolution 68/167; and A/HRC/32/38). The Human Rights Committee, previous mandate holders and the Special Rapporteur have examined States' obligations under article 19 of the Covenant. In short, States may not interfere with, or in any way restrict, the holding of opinions (see art. 19 (1) of the Covenant; and A/HRC/29/32, para. 19). Article 19 (3) of the Covenant provides that States may limit freedom of expression only where provided by law and necessary for the 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 or morals (see Human Rights Committee general comment No. 34 (2011); A/71/373; and A/HRC/29/32).

6. States also have obligations to take steps to protect individuals from undue interference with human rights when committed by private actors (see art. 2 (2) of the Covenant; and Human Rights Committee general comment No. 31 (2004)). Human rights law protects individuals against violations by the State as well as abuses committed by private persons or entities (see general comment No. 31, para. 8).[4] The Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, endorsed by the Human Rights Council in 2011, explains that States are required to take appropriate steps to prevent, investigate, punish and redress private actors' abuse (see A/HRC/17/31, annex, principle 1). Such steps include the adoption and implementation of legislative, judicial, administrative, educative and other appropriate measures that require or enable business respect for freedom of expression, and, where private sector abuses occur, access to an effective remedy (see general comment No. 31, para. 7; and A/HRC/17/31, annex, principles 3 and 25).

7. The government actions described below often fail to meet the standards of human rights law. Moreover, a lack of transparency pervades government interferences with the digital access industry. Failures of transparency include vague laws providing excessive discretion to authorities, legal restrictions on third party disclosures concerning government access to user data and specific gag orders. The lack of transparency undermines the rule of law as well as public understanding across this sector.[5]

A. Internet and telecommunications shutdowns

8. Internet and telecommunications shutdowns involve measures to intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law (see A/HRC/32/13, para. 10).[6] Governments typically conduct or order shutdowns, often with the assistance of private actors that operate networks or facilitate network traffic. Large-scale attacks on network infrastructure committed by private parties, such as distributed denial-of-service (DDoS) attacks, may also have shutdown effects. While shutdowns are frequently associated with total network outages, they may also arise when access to mobile communications, websites or social media and messaging

[4] See also African Commission on Human and Peoples' Rights, general comment No. 3 (2015) on the right to life, para. 38; Inter-American Court of Human Rights, *Velásquez Rodríguez Case*, judgment of 29 July 1988, para. 172; and European Court of Human Rights, *Özel and others v. Turkey*, judgment of 17 November 2015, para. 170.

[5] Freedom Online Coalition, Report of Working Group 3: Privacy and Transparency Online, November 2015.

[6] Access Now recorded 15 shutdowns in 2015 and 56 shutdowns in 2016. The first recorded shutdown reportedly occurred in Nepal in February 2005.

applications is blocked, throttled or rendered "effectively unusable".[7] Shutdowns may affect towns or regions within a country, an entire country or even multiple countries and may last for periods ranging from hours to months.

9. Shutdowns ordered covertly or without an obvious legal basis violate the requirement of article 19 (3) of the Covenant that restrictions be "provided by law". In Chad, the failure of authorities to provide a meaningful public explanation for a series of Internet and social media shutdowns between February and October 2016 created the presumption that they were unlawful.[8] In Gabon, total network outages were allegedly recorded every evening for almost two weeks during the 2016 election period, contrary to government assurances that such services would not be disrupted.[9]

10. Shutdowns ordered pursuant to vaguely formulated laws and regulations also fail to satisfy the legality requirement. In Tajikistan, the amended Law on the State of Emergency authorizes the Government to block mobile services and Internet access without a court order following the declaration of a state of emergency.[10] The law fails to define when and for what purposes a state of emergency may be declared. Such ambiguity enables authorities' unfettered discretion to implement shutdowns. In some countries, authorities rely on antiquated laws to justify shutdowns.[11] Laws and regulations adopted and implemented in secret also violate the legality requirement. In the United States of America, the National Coordinating Center for Telecommunications has largely redacted public release of standard operating procedure 303, an executive regulation that establishes "detailed procedures" on the "disruption of cellular service."[12] While these procedures have not been publicly invoked, the potential for authorities to evade legal scrutiny and public accountability runs contrary to article 19 of the Covenant.

11. Restrictions on expression must be necessary to achieve aims specified by article 19 (3) of the Covenant and may never be invoked to justify the suppression of advocacy for democratic rights (see Human Rights Committee general comment No. 34, para. 23; and A/71/373, para. 26). However, governments frequently impose shutdowns during demonstrations, elections and other events of extraordinary public interest, with little or no explanation.[13] In Bahrain, disruptions to mobile and Internet access in Duraz allegedly coincided with sit-ins outside the home of a prominent religious leader whose citizenship the Government had revoked.[14] Internet users in the Bolivarian Republic of Venezuela were reportedly denied Internet access during widespread protests against the Government in 2014.[15] Network disruptions have been recorded during or around elections or protests in

[7] Access Now submission, part I, p. 1.
[8] Internet Sans Frontières submission, p. 2, TCD 3/2016.
[9] Ibid., GAB 1/2016.
[10] OHCHR, "Preliminary observations by the United Nations Special Rapporteur on the right to freedom of opinion and expression, Mr. David Kaye, at the end of his visit to Tajikistan, press release (9 March 2015).
[11] India, Code of Criminal Procedure, sect. 144; also Apar Gupta and Raman Jit Singh Chima, "The cost of internet shutdowns", *The Indian Express* (26 October 2016).
[12] United States of America, NCC Standard Operating Procedure (SOP) 303.
[13] Access Now submission, part I, pp. 5-7.
[14] Bahrain Center for Human Rights, *Digital Rights Derailed in Bahrain* (2016), pp. 13-14.
[15] Danny O'Brien, "Venezuela's Internet crackdown escalates into regional blackout", Electronic Frontier Foundation (20 February 2014).

Cameroon,[16] the Gambia,[17] India,[18] Myanmar,[19] the Islamic Republic of Iran,[20] Uganda[21] and Montenegro.[22]

12. The failure to explain or acknowledge shutdowns creates the perception that they are designed to suppress reporting, criticism or dissent. Reports of repression and State-sanctioned violence in the wake of network disruptions have led to allegations that some States exploit the darkness to commit and cover up abuses. In Sudan, for example, Internet access was shut down for several hours during a deadly crackdown on demonstrators protesting fuel price hikes in September 2013.[23]

13. Observers have also noted the growing use of shutdowns to prevent cheating by students during national exams. Uzbekistan may have been the first to invoke this justification during university entrance exams in 2014.[24] In 2016, authorities allegedly ordered shutdowns during exams in India, Algeria, Ethiopia and Iraq.[25]

14. Network shutdowns invariably fail to meet the standard of necessity. Necessity requires a showing that shutdowns would achieve their stated purpose, which in fact they often jeopardize. Some governments argue that it is important to ban the spread of news about terrorist attacks, even accurate reporting, in order to prevent panic and copycat actions.[26] Yet it has been found that maintaining network connectivity may mitigate public safety concerns and help restore public order. During public disturbances in London in 2011, for example, authorities used social media networks to identify perpetrators, disseminate accurate information and conduct clean-up operations. In Kashmir, police have reported on the positive role of mobile phones in locating people trapped during terrorist attacks. [27]

15. Duration and geographical scope may vary, but shutdowns are generally disproportionate. Affected users are cut off from emergency services and health information, mobile banking and e-commerce, transportation, school classes, voting and election monitoring, reporting on major crises and events, and human rights investigations. [28] Given the number of essential activities and services they affect, shutdowns restrict expression and interfere with other fundamental rights.

16. Shutdowns also affect areas beyond those of specific concern.[29] In the lead up to the 2015 National Day Parade in Pakistan, mobile communications networks were allegedly cut off at the parade site as well as in surrounding areas that were not expected to experience any potential security threat.[30] During the Pope's visit to the Philippines in 2015, the shutdown of mobile networks for safety reasons affected areas well beyond the travel

[16] OHCHR, "UN expert urges Cameroon to restore Internet services cut off in rights violation", press release (10 February 2017).
[17] Deji Olukotun, "Gambia shuts down Internet on eve of elections", Access Now (30 November 2016).
[18] Software Freedom Law Center, "Internet shutdowns in India, 2013-2016".
[19] Freedom House, "Freedom on the Net: Myanmar" (2011).
[20] Center for Democracy and Technology, "Iran's Internet throttling: unacceptable now, unacceptable then" (3 July 2013).
[21] Article 19, "Uganda: Blanket ban on social media on election day is disproportionate" press release (18 February 2016).
[22] Global Voices, "WhatsApp and Viber blocked on election day in Montenegro" (17 October 2016).
[23] Human Rights Watch, "Sudan: Dozens killed during protests" (27 September 2013).
[24] Access Now submission, part I; also Freedom House, "Freedom on the Net: Uzbekistan" (2016).
[25] Access Now submission, part I.
[26] See for example, OHCHR, "Preliminary conclusions and observations by the UN Special Rapporteur on the right to freedom of opinion and expression to his visit to Turkey, 14-18 November 2016", press release (18 November 2016).
[27] Institute for Human Rights and Business (IHRB), "Security v. Access: The impact of mobile network shutdowns", case study: Telenor Pakistan (September 2015), pp. 31-32.
[28] Access Now submission, part I, pp. 11-14; also Global Network Initiative submission.
[29] IHRB, "Security v. Access: The impact of mobile network shutdowns", case study: Telenor Pakistan (September 2015), p. 20.
[30] Ibid., pp. 27-28.

route.[31] When specific services or platforms are disrupted, governments typically target those that are the most efficient, secure or widely used.[32]

B. Government access to user data

17. Government surveillance today relies on access to communications and associated data belonging to users of privately owned networks. While such access frequently requires the assistance of private actors, it may also be obtained without their knowledge or involvement. As with other forms of surveillance, government access to user data may interfere with privacy in a manner that can both directly and indirectly limit the free development and exchange of ideas (see A/HRC/23/40, para. 24). Undue access to personal data implicitly warns users to think twice and possibly avoid controversial viewpoints, the exchange of sensitive information and other exercises of freedom of expression that may be under government scrutiny (see A/HRC/27/37, para. 20).

Requests for user data

18. Vague laws and regulations violate the legality requirement (see A/HRC/23/40, para. 50). The Communications and Multimedia Act of Malaysia, for example, permits authorities to order the disclosure of "any communication or class of communications" on "the occurrence of any public emergency or in the interest of public safety". The Act does not define the conditions that trigger a public emergency and certification by the King is deemed "conclusive proof on the point".[33] In Qatar, law enforcement enjoys a broad right to seek access to providers' customer communications in cases of national security or emergency.[34] These provisions empower authorities to request user data based on a mere assertion of national security. Users are thus unable to predict with reasonable certainty the circumstances under which their communications and associated data may be disclosed to authorities.

19. Providers should only be compelled to release user data when ordered by judicial authorities certifying necessity and proportionality to achieve a legitimate objective. The Criminal Code of Canada requires law enforcement to submit requests for the disclosure of telephone records in criminal investigations to a judge for approval.[35] In Portugal, the authorities must obtain a judicial order to compel the disclosure of communications data.[36] However, national law often exempts user data requests from judicial authorization. In Bangladesh, the authorities require only executive branch approval to access communications data belonging to telecommunications subscribers on the grounds of national security and public order.[37]

20. Laws that require private actors to create large databases of user data accessible to the government raise necessity and proportionality concerns. In Kazakhstan, telephone numbers, e-mail and Internet Protocol (IP) addresses and billing information must be stored by the provider for two years.[38] The Russian Federation requires private actors to store the content of all their customers' calls and text messages for six months, and related communications metadata for three years.[39] Both countries also require such data to be stored locally.[40] In countries where mobile phones are a dominant means of communication, mandatory SIM card registration laws effectively require the majority of the population to divulge personally identifiable information (see A/HRC/29/32, para. 51).

[31] Deniz Duru Aydin, "Five excuses governments (ab)use to justify Internet shutdowns" Access Now (6 October 2016).
[32] Article 19 submission, p. 2.
[33] Malaysia, Communications and Multimedia Act (1998), sect. 266.
[34] Qatar, Decree Law No. (34) of 2006.
[35] See submission from Canada, p. 6.
[36] Portugal, Criminal Proceedings Code, arts. 187-190.
[37] Bangladesh, Telecommunication Regulatory Act (2001), sect. 97 (Ka).
[38] Kazakhstan, Government resolution No. 1593 (23 December 2011).
[39] OHCHR, letter to the Government of the Russian Federation, 28 July 2016 (OL RUS 7/2016).
[40] Article 19 submission, p. 5.

The mandatory retention of large amounts of user data runs contrary to established due process standards, such as the need for individualized suspicion of wrongdoing.

Undermining encryption

21. Since the Special Rapporteur's report on encryption and anonymity (A/HRC/29/32), unnecessary and disproportionate measures to undermine encryption have increased globally and threaten to undermine both the freedom of expression and digital security of users. In the United Kingdom of Great Britain and Northern Ireland, for example, the 2016 Investigatory Powers Act permits the Secretary of State to issue "technical capability notices" that require providers to remove "electronic protection" from communications — a measure that could compel backdoors or otherwise limit or weaken encryption.[41] States have not provided sufficient evidence that such vulnerabilities are the least intrusive means of protecting national security and public order, particularly given the breadth and depth of other investigative tools at their disposal (Ibid., para. 39).

Direct access

22. Direct access to Internet and telecommunications networks enables authorities to intercept and monitor communications with limited legal scrutiny or accountability. Technological advances have enhanced the ability of law enforcement and intelligence agencies to obtain a direct connection to networks without the involvement or knowledge of the network operator.[42] During the 2014 general election in the former Yugoslav Republic of Macedonia, intelligence authorities allegedly obtained direct access to the country's major telecommunications networks to intercept the communications of over 20,000 people, including politicians, activists, government officials and journalists. Many targets were also sent a transcript of their phone calls.[43] In India, it appears that authorities are developing a Central Monitoring System programme that would enable "electronic provisioning of target numbers by government agency without any manual intervention from telecommunications service providers on a secure network."[44] These activities do not appear to be provided by law, lacking both judicial authorization and external oversight. Furthermore, the risks they pose to the security and integrity of network infrastructure raise proportionality concerns.

C. Net neutrality

23. Network neutrality — the principle that all Internet data should be treated equally without undue interference — promotes the widest possible access to information.[45] In the digital age, the freedom to choose among information sources is meaningful only when Internet content and applications of all kinds are transmitted without undue discrimination or interference by non-State actors, including providers. The State's positive duty to promote freedom of expression argues strongly for network neutrality in order to promote the widest possible non-discriminatory access to information.

Paid prioritization

24. Under paid prioritization schemes, providers give preferential treatment to certain types of Internet traffic over others for payment or other commercial benefits. These schemes effectively create Internet fast lanes for content providers that can afford to pay extra and slow lanes for all others.[46] This hierarchy of data undermines user choice. Users

[41] United Kingdom of Great Britain and Northern Ireland, Investigatory Powers Act (2016), art. 253; also OHCHR, letter to the Government of the United Kingdom, 22 December 2015 (AL GBR 4/2015).

[42] Privacy International submission; and Telecommunications Industry Dialogue submission, p. 3.

[43] Privacy International, "Macedonia: Society On Tap" (23 March 2016).

[44] Access Now submission, part II, p. 4.

[45] Luca Belli submission; and Article 19 submission, pp. 7-8.

[46] Dawn C. Nunziato and Arturo J. Carrillo, "The price of paid prioritization: The international and domestic consequences of the failure to protect Net neutrality in the United States", Georgetown

experience higher costs or lower quality of service when they attempt to access Internet content and applications in the slow lanes. At the same time, they may be compelled to engage with content that has been prioritized without their knowledge or input.

25. Several States prohibit paid prioritization. For example, the Netherlands, an early adopter of net neutrality, forbids providers from making "the price of the rates for Internet access services dependent on the services and applications which are offered or used via these services".[47] The United States Federal Communications Commission 2015 Open Internet Order bans the "management of a broadband provider's network to directly or indirectly favour some traffic over other traffic ... in exchange for consideration (monetary or otherwise) from a third party, or to benefit an affiliated entity".[48]

Zero rating

26. Zero rating is the practice of not charging for the use of Internet data associated with a particular application or service; other services or applications, meanwhile, are subject to metered costs. Zero rating arrangements vary from data plans that exempt certain Internet services from a subscriber's usage count to the provision of unmetered access to certain services without the purchase of a plan.[49] Variations notwithstanding, zero rating arrangements privilege access to content and may increase the cost of metered data. For users who struggle to afford metered data, they might end up relying exclusively on zero-rated services, resulting in limited access to information for communities that may already be marginalized in their access to information and public participation.

27. Zero rating arrangements may provide users with limited Internet access in areas that would otherwise completely lack access.[50] However, broader Internet access may still remain out of reach for users, trapping them in permanently walled online gardens.[51] The assumption that limited access will eventually ripen into full connectivity requires further study. It may be dependent upon factors such as user behaviour, market conditions, the human rights landscape and the regulatory environment.[52]

28. These competing considerations have led to variations in regulatory approaches. In India, public concern over Facebook's Free Basics culminated in a ban on any arrangement that "has the effect of discriminatory tariffs for data services being offered or charged to the consumer on the basis of content".[53] Restrictions on zero rating are in effect in Chile, Norway, the Netherlands, Finland, Iceland, Estonia, Latvia, Lithuania, Malta and Japan.[54] In contrast, the United States, followed later by the Body of European Regulators for Electronic Communications (BEREC), adopted guidelines involving a case-by-case approach.[55] States that adopt a case-by-case approach should carefully scrutinize and, if necessary, reject arrangements that, among other things, zero-rate affiliated content, condition zero rating on payment or favour access to certain applications within a class of

Journal of International Affairs: International Engagement on Cyber V: Securing Critical Infrastructure (2 October 2015), p. 103.

47 Netherlands, Telecommunications Act, art. 7.4a (3).

48 United States of America, Federal Communications Commission, Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 18. This Order, possibly under threat at the time of writing the present report, remains a useful template for net neutrality regulation.

49 Erik Stallman and R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms", Center for Democracy and Technology (January 2016).

50 Ibid., pp. 4 and 11.

51 Barbara van Schewick, "Network neutrality and zero-rating", submission to the United States Federal Communications Commission (19 February 2014), p. 7.

52 Erik Stallman and R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms" (January 2016), p. 15.

53 India, Telecom Regulatory Authority, "TRAI releases the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016", press release (8 February 2016).

54 Emily Hong, "A zero sum game? What you should know about zero-rating", *New America Weekly*, Edition 109 (4 February 2016).

55 United States, Federal Communications Commission, Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 21; and BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (August 2016) (BoR (16) 127).

similar applications (for example, zero rating certain music streaming services rather than all music streaming). Additionally, States should require meaningful corporate disclosures about network traffic management practices. For example, Chile requires ISPs to disclose Internet access speeds, price or speed differentials between national and international connections, and related service guarantees.[56]

III. Digital access providers and freedom of expression

29. While the duty of States to respect and protect freedom of expression is well-established, the private actors that establish, operate and maintain digital access also play a critical role.

A. Telecommunications and Internet service providers

30. Telecommunications providers (Telcos) and ISPs (collectively referred to in the present report as "providers") offer a diverse range of services. While they principally operate and sell access to the series of networks that comprise the Internet, they also enable users to communicate and share information through mobile services and traditional landlines (see A/HRC/32/38, para. 16). While providers remain State-owned in many regions, a growing number are now privately established and managed. The industry is also increasingly multinational: some of the world's biggest providers operate networks in multiple countries and regions, often through partnerships with domestic companies or their own subsidiaries.

31. As gatekeepers of vast information networks, providers face significant government pressure to comply with censorship and surveillance activities. To operate a network in a country, they are required to invest substantial physical and business infrastructure, including network equipment and personnel. They are typically subject to local law and other licensing requirements set out in agreements with the State. In addition to legal pressure, providers have also faced extralegal intimidation, such as threats to the safety of their employees and infrastructure in the event of non-compliance.[57]

32. While several providers attempt to resist censorship and surveillance requests, many assist in government efforts without meaningful challenge. In the United States, one of the country's largest providers is alleged to have created a "super search engine" to facilitate law enforcement access to customer phone calls, even though not legally required to do so.[58] In the United Kingdom, a complaint filed with the Organization for Economic Cooperation and Development alleged that major providers granted the country's intelligence agency access to their networks and customer data well beyond what was required by the law at the time.[59]

33. A growing number of providers are establishing arrangements with media and other content-producing companies that threaten net neutrality and are lobbying intensely for concessions on net neutrality standards. For example, as European regulators were developing net neutrality guidelines, 17 major providers in the region issued the "5G Manifesto", warning that "excessively prescriptive" guidelines would delay their investment in 5G, the next generation of mobile Internet connection.[60]

[56] Chile, Ley No. 20.453, art. 24 H (D).

[57] Telecommunications Industry Dialogue submission, p. 10.

[58] Dave Maass and Aaron Mackey, "Law enforcement's secret 'super search engine' amasses trillions of phone records for decades", Electronic Frontier Foundation (29 November 2016).

[59] Privacy International, "OECD complaint against BT, Verizon Enterprise, Vodafone Cable, Viatel, Level 3, and Interoute".

[60] Article 19 submission, p. 9.

B. Internet exchange points

34. IXPs enable the exchange of Internet traffic between and among networks managed by different providers within a country or region.[61] This form of interconnection prevents local or regional Internet traffic from taking long and circuitous international routes, thus enhancing the speed and efficiency of Internet connectivity. IXPs may be established by Internet infrastructure companies as part of a broader suite of services sold to providers or operated as non-profit or volunteer organizations.[62]

35. IXPs handle an enormous volume of Internet traffic that may be filtered or intercepted at government request. The growing number of censorship and surveillance incidents involving IXPs indicates that they are major access choke points, even if their precise role is unclear. For example, in 2013, the manner in which access to YouTube was blocked in Pakistan indicated that the platform was filtered by IXPs, rather than ISPs, through a method known as "packet injection".[63] According to a leaked internal memo of a multinational ISP operating in Ecuador, users were unable to access Google and YouTube in March 2014 because the private Association of Internet Providers of Ecuador — which runs two of the major IXPs in the country — was "blocking access to certain Internet websites by request of the national Government".[64] The revelations of mass surveillance conducted by the United States National Security Agency have raised concern among technologists that the agency is intercepting a significant proportion of domestic and foreign Internet traffic by targeting United States IXPs.[65] In September 2016, the world's largest Internet exchange point, which is based in Germany, challenged legal orders issued by the country's intelligence agency to monitor international communications transiting through its hub.[66]

C. Content delivery networks

36. A content delivery network (CDN) is a network of servers strategically distributed around the world to enable the efficient delivery of web pages and other Internet content. Large content producers rely on content delivery networks to reach as many users as quickly as possible.[67] A content delivery network stores copies of content hosted on these platforms and redirects a user's request for such content from the platform's servers to the servers within its network that are located closest to the user.[68] This process enhances the speed of content delivery, particularly to users located far away from the platform's servers. Content delivery networks are regarded as an effective safeguard against website blocking; censorship measures targeting servers that host a particular website or platform do not affect the content delivery network's delivery of copies of the same content to users.[69] Content delivery networks have also become a critical bulwark against network disruptions. The demands of rapid access have incentivized them to invest significant resources in infrastructure and services that can withstand distributed denial-of-service and other malicious attacks.[70]

---

[61] See www.bgp4.as/internet-exchanges/.

[62] Jason Gerson and Patrick Ryan, "A primer on Internet exchange points for policymakers and non-engineers" *Social Science Research Network* (12 August 2012), p. 10.

[63] Zubair Nabi, "The anatomy of web censorship in Pakistan" (2013), p. 4.

[64] Katitza Rodriguez, "Leaked documents confirm Ecuador's Internet censorship machine", Electronic Frontier Foundation (14 April 2016).

[65] Andrew Clement and Jonathan Obar, "Canadian Internet 'boomerang' traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges", in *Law, Privacy and Surveillance in Canada in the Post-Snowden Era,* Michael Geist, ed. (University of Ottawa Press, 2015).

[66] De Cix, "Information on the lawsuit against the Federal Republic of Germany" (16 September 2016).

[67] Geoff Huston, "The death of transit?", Asia Pacific Network Information Centre (27 October 2016).

[68] Vangie Beal, "CDN – Content Delivery Network", *Webopedia*.

[69] John Holowczak and Amir Houmansadr, "CacheBrowser: bypassing Chinese censorship without proxies using cached content" (2015).

[70] Geoff Huston, "The death of transit?", Asia Pacific Network Information Centre (27 October 2016).

37. The censorship resilience of content delivery networks has also made them targets of disproportionate restrictions on freedom of expression. In Egypt, the blocking of *The New Arab* website in August 2016 also disrupted access to content on other sites that, although unaffiliated, shared the same content delivery network, which led researchers to believe authorities had targeted that particular network.[71] In China, a national filter has reportedly blocked EdgeCast content delivery network, which handles content for a number of large websites in the country.[72]

38. Since content delivery networks process large volumes of user requests for Internet content from multiple websites and platforms, they are also vulnerable to government surveillance. In 2016, for example, Amazon Web Services, which houses one of the world's biggest content delivery networks,[73] reported that government requests to access data more than doubled from the previous year.[74] Researchers also believe that mass surveillance activities strategically target content delivery networks to maximize information collection, but specifically how this is conducted and the extent of content delivery network involvement, if any, is unclear.[75]

D. Network equipment vendors

39. Vendors supply the hardware and software that form the basis of Internet and telecommunications networks. Network equipment typically includes routers, switches and access points, which enable multiple devices and networks to connect with each other (see A/HRC/32/38, para. 18). Vendors have also diversified their business to provide Voice over Internet Protocol (VoIP) equipment, which enables wireless calls and Internet of Things (IoT) technology, which enables networking among smart devices.[76] Vendors are rarely consumer-facing: their main customers are network operators, such as governments, ISPs, or content delivery networks. As a result, they are required to configure networks to the technical standards specified by these operators, including standards dictated by local law (such as law enforcement and national security requirements). However, vendors may also design or modify equipment and technology to ensure consistency with private or government specifications.

40. Given their business model, vendors are required to navigate the human rights challenges that their customers face or create. In the area of surveillance, vendors are often bound by "lawful interception" measures, which require the configuration of networks to enable government access to user data.[77] Additionally, vendors may be contracted to establish "administration and mediation systems" that facilitate the sharing of intercepted data between the network operator and the government authority as well as the government systems that process the intercepted data.[78] In arrangements where vendors also manage the networks that they have built, they may also be responsible for handling government requests for user data on the operator's behalf.[79]

[71] Leonid Evdokimov and Vasilis Ververis, "Egypt: Media censorship, Tor interference, HTTPS throttling and ads injections?", Open Observatory of Network Interference (27 October 2016).

[72] Joss Wright, "A quick investigation of EdgeCast CDN blocking in China", blog, Oxford Internet Institute (18 November 2014).

[73] At the time of writing the present report, Amazon Cloudfront served the largest number of website domains in the world.

[74] Amazon Information Request Report (June 2016).

[75] See, for example, Harrison Weber, "How the NSA & FBI made Facebook the perfect mass surveillance tool", *Venture Beat* (15 May 2014).

[76] Michael E. Raynor and Phil Wilson, "Beyond the dumb pipe: The IoT and the new role for network service providers", Deloitte University Press (2 September 2015).

[77] See, for example, Council of the European Union resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal C 329; and Privacy International submission, pp. 2-3.

[78] IHRB, "Human rights challenges of telecommunications vendors: addressing the possible misuse of telecommunications systems: case study: Ericsson" (November 2014), p. 16.

[79] Ibid., p. 17.

41. The design of network equipment and technology with multiple uses raises freedom of expression and privacy concerns. Deep packet inspection devices, for example, are used for innocuous technical purposes such as the management of network congestion, but have also been employed to filter Internet content, intercept communications and throttle data flows. Mobile networks are configured to monitor the real-time location of cell phones to ensure that cellular services may be accessed from any location, but such monitoring may also be used to target users.[80]

42. Some evidence suggests that vendors may provide support for government censorship and surveillance. In a case pending before United States courts, Cisco has been accused of designing, implementing and helping to maintain a Chinese surveillance and internal security network known as the Golden Shield.[81] (Cisco denies those allegations.)[82] In Ethiopia, human rights groups found that ZTE Corporation had designed and installed a customer management database for Ethio Telecom that enabled intrusive surveillance.[83]

E. Other private actors

43. The findings and recommendations in the present report apply to any entity that engages in the provision of digital access as described above. A growing number of Internet companies are adding critical digital access and infrastructure services to their portfolio. For example, Alibaba and Tencent, two of the biggest Chinese Internet companies, now also offer content delivery network services.[84] Google has been experimenting with methods to provide wireless access that bypass traditional providers; in 2010, it launched a high-speed Internet connection service to homes and businesses in select cities in the United States.[85] It is also working with Facebook and Microsoft to build undersea cable networks that would enable them to connect users without relying on third-party equipment or systems.[86]

44. Standards developing organizations (SDOs), although not strictly "industry actors", establish technical protocols and standards that enable inter-operability in the telecommunications and Internet infrastructure. Standards development that neglects human rights considerations may adversely impact freedom of expression. For example, the failure to mandate Transport Layer Security (TLS) as a feature of the Hypertext Transfer Protocol (HTTP) left web traffic vulnerable to censorship and surveillance. The technical community's efforts to incorporate human rights due diligence into standards development is therefore a step in the right direction.[87]

IV. Human rights responsibilities of digital access providers

45. The Guiding Principles on Business and Human Rights recognize the responsibility of business enterprises to respect human rights, independent of State obligations or the implementation of those obligations (see A/HRC/17/31, annex; and A/HRC/32/38, paras. 9-10). They provide a minimum baseline for corporate human rights accountability, urging companies to adopt public statements of commitment to respect human rights endorsed by

[80] Ibid., p. 13.

[81] United States District Court for the Northern District of California, San Jose Division, *Doe et al. v. Cisco Systems, Inc. et al.*, Case No. 5:11-cv-02449-EJD-PSGx (18 September 2013).

[82] John Earnhardt, "Cisco Q&A on China and censorship" Cisco blogs (2 March 2006).

[83] Human Rights Watch, "They know everything we do: telecom and Internet surveillance in Ethiopia" (25 March 2014).

[84] Tencent Cloud CDN and Alibaba Cloud CDN.

[85] Klint Finley, "Google eyes blazing-fast wireless as a way into your home", *Wired* (12 August 2016).

[86] Joon Ian Wong, "Google and Facebook are doubling down on Internet infrastructure with a new Pacific cable", *Quartz* (17 October 2016).

[87] Internet Research Task Force, "Research into human rights protocol considerations" (25 February 2017). Available at https://datatracker.ietf.org/doc/draft-irtf-hrpc-research/?include_text=1. The supplementary annex analyzes the roles and responsibilities of standards developing organizations in more detail.

senior or executive-level management; conduct due diligence processes that meaningfully "identify, prevent, mitigate and account for" actual and potential human rights impacts throughout the company's operations; and provide for or cooperate in the remediation of adverse human rights impacts (see A/HRC/17/31, annex, principles 16-24).

A. Context considerations

46. The Guiding Principles emphasize the need for companies to take into account the particularities of their operating context when executing their human rights responsibilities (Ibid.). In the digital access industry, several contexts must be considered.

Access providers supply a public good

47. The digital access industry is in the business of digital expression; its commercial viability depends on users who seek, receive and impart information and ideas on the networks it builds and operates. Since privately owned networks are indispensable to the contemporary exercise of freedom of expression, their operators also assume critical social and public functions. The industry's decisions, whether in response to government demands or rooted in commercial interests, can directly impact freedom of expression and related human rights in both beneficial and detrimental ways.

Restrictions on Internet access affect freedom of expression globally

48. The industry's human rights impacts are frequently global, affecting users even in markets beyond those served by the company concerned. For example, surveillance of a single Internet exchange point in the United States may capture large streams of communications among Americans and foreigners, and even those entirely among foreigners. Similarly, security vulnerabilities in network design affect all users who rely on the compromised network for digital access, including users located far away from the network. Accordingly, companies should identify and address the broader implications of their activities for freedom of expression generally, in addition to their impacts on customers or rights holders in the markets they operate. To be sure, the manner in which they account for their impacts may vary according to their size, resources, ownership, structure and operating context (Ibid., principle 14). For example, all providers should vet user data requests for compliance with a minimum set of formalities, regardless of the origin of the request or the user affected. But while a multinational provider may have dedicated teams vetting requests, a small or medium-size provider may task its legal or public policy teams to perform the same function.

The industry is vulnerable to State pressure against freedom of expression…

49. The Guiding Principles seek to address the gaps in corporate accountability left because of a lack of national legislation or implementation. [88] However, zealous enforcement of domestic law also poses human rights challenges in the digital access industry. For example, States may hold providers liable for, or otherwise pressure them to restrict, Internet content posted by users on their networks, under laws as varied as hate speech, defamation, cybercrime and lese-majesty. Yet such intermediary liability creates a strong incentive to censor: providers may find it safest not to challenge such regulation but to over-regulate content such that legitimate and lawful expression also ends up restricted. The pressure to assist in State censorship and surveillance also escalates when authorities harass, threaten or arrest employees, or attempt to tamper with the company's networks or equipment.[89]

[88] Yael Ronen, "Big Brother's little helpers: the right to privacy and the responsibility of Internet service providers", *Utrecht Journal of International and European Law*, vol. 31, No. 80 (February 2015), p. 76.

[89] In 2014, a network shutdown request that the multinational telecommunications provider, Orange, received from the authorities in the Central African Republic was reportedly "accompanied by the

...but also uniquely situated to ensure respect for users' rights

50. The industry's dual role as an enabler of digital access and a natural point for State-imposed restriction heightens its importance as a bulwark against government and private overreach. For example, providers are usually best placed to push back on a shutdown or user data request. Content delivery networks are strategically positioned on the Internet infrastructure to counter malicious attacks that disrupt access. Vendors are uniquely qualified to assess whether their products will be or are being used to facilitate human rights abuses, particularly when they conduct sales due diligence or perform ongoing services.

B. Responsibility to respect users' freedom of expression

51. To operationalize its human rights commitments, the digital access industry should allocate appropriate resources to at least the practices described below. Although these principles are evaluated in the context of digital access, they also bear relevance to other sectors of the digital economy, such as social media, commerce, surveillance and search.

1. Due diligence

52. Due diligence processes enable a digital access provider to identify, prevent and mitigate the human rights impacts of its activities (see A/HRC/17/31, annex, principle 19). While one-size-fits-all due diligence approaches are neither possible nor advisable, human rights impact assessments provide a means of assessing and addressing risks to freedom of expression and privacy.[90] Due diligence involves at least the following.

Policies governing the conduct of due diligence

53. Companies should develop clear and specific criteria for identifying activities that implicate freedom of expression and trigger due diligence processes.[91] The company's past and ongoing human rights effects, as well as industry practice, provide useful indicators. In the digital access industry, such activities might include mergers and acquisitions; market entry or exit; government or non-government requests for content restriction or user data; the development of or changes to content restriction and privacy policies; product changes regarding content moderation or encrypted communications; arrangements that facilitate prioritized access to Internet content and applications; the design, sale and purchase of network interception and filtering equipment and technologies as well as associated training and consultation services.[92] This list, which is far from exhaustive, "requires constant vigilance and updating", taking into account new areas of business, developments in technology, and other changes in operating context.[93]

Issues to examine

54. Due diligence processes should critically examine at least applicable local and international laws and standards, including potential conflicts between local laws and human rights; freedom of expression and privacy risks embedded in the company's products and services; strategies to mitigate and prevent these risks; limits on the effectiveness of these strategies given the company's legal, regulatory or operating

threat of personal sanctions in case of non-compliance". See Telecommunications Industry Dialogue submission, p. 11.

[90] Major telecommunications providers that have developed human rights impact assessments include Telia Company and Telefonica. Ibid., pp. 7-8.

[91] Nokia has embedded an automated feature that flags potential sales for human rights risks in its sales tool. Ibid., p. 7.

[92] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pp. 32-36.

[93] Michael A. Samway, "Business, human rights and the Internet: a framework for implementation", in *Human Dignity and the Future of Global Institutions*, Mark P. Lagon and Anthony Clark Arend, eds. (Washington, D.C., Georgetown University Press, 2014), p. 308.

environment; and the potential to promote human rights throughout the company's operations.[94]

Internal process and training

55. While dedicated business and human rights professionals within a company are important, due diligence should not be solely their responsibility, but must involve other relevant functional groups within the business. This requires dialogue and collaboration among various business units (such as privacy, law enforcement, government relations, compliance, risk management, product development and operations) and professionals (such as engineers, user-experience researchers, sales teams and business executives).[95] In the privacy context, researchers have found that measures such as "involving and assigning responsibility to senior business unit executives" for privacy management and "embedding staff with privacy protection expertise and personal responsibility for privacy … into the business units", create an environment conducive to privacy protection.[96] Similar management practices could also ensure business respect for freedom of expression. For small and medium-size enterprises, these considerations might require the entire operation to engage in due diligence activities.[97]

External expertise

56. Given the wide knowledge base required, due diligence processes should draw on external, non-governmental expertise, including local civil society, international human rights organizations, the human rights mechanisms of international and regional organizations, academia and the technical community. Multi-stakeholder fora also provide opportunities for shared learning and mutual accountability. For example, researchers have found that membership in sector- or industry-specific human rights initiatives, such as the Global Network Initiative and the Telecommunications Industry Dialogue, coincides with companies' human rights performance.[98]

Consultation with users and affected rights holders

57. All digital access providers implicate the freedom of expression of end users in one way or another. Accordingly, even companies that are not consumer facing should consult end users as part of their risk assessment process. Such consultation is distinguishable from the broader multi-stakeholder engagement efforts outlined above and contemplates a "two-way dialogue" to "gather specific views or advice from affected stakeholders (or their representatives) that are then taken into account in the company's internal decision-making and implementation processes".[99] For example, vulnerable or marginalized individuals and groups might be consulted while licensing negotiations in high-risk operating environments are ongoing or during the design, testing and rollout of zero rating policies. Meaningful consultation should also involve regular outreach to civil society organizations, which may provide a useful proxy for the needs and interests of end users in particular communities, and might themselves be at greater risk of pressure for their advocacy.

Ongoing dynamic assessments

58. Companies should be quick to adapt due diligence processes to changes in circumstances or operating context. For example, risk assessment should continue after the

[94] Ibid., pp. 310-312, for a more comprehensive overview of relevant topic areas that due diligence processes should cover.

[95] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 36.

[96] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, Massachusetts, MIT Press, 2015), p. 177.

[97] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 37.

[98] Ranking Digital Rights submission, p. 5.

[99] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pp. 37-38.

design phase and at regular intervals throughout the life cycle of the product or service, taking into account factors such as technology and infrastructure changes and associated security vulnerabilities, alterations in consumer behaviour, and modifications of the legal, political and social environment where companies operate.[100]

2. Incorporating human rights safeguards by design

59. As with every major technology development, design and engineering choices reflect public policy considerations, and should be guided by respect for human rights. For example, network slicing, a key 5G technology, could enable mobile providers to manage network traffic more efficiently and cater to the ever-expanding range of consumer needs in the Internet of Things (IoT) era. At the same time, networks could also be "sliced" into fast and slow lanes that prioritize access to some Internet applications over others, potentially interfering with net neutrality. Accordingly, companies should ensure that innovations in network equipment and technology — particularly those with multiple uses — are designed and deployed so as to be consistent with freedom of expression and privacy standards.[101]

60. Companies should assume an active and engaged role in developing expression and privacy enhancing measures. For example, digital security measures that detect and prevent distributed denial-of-service attacks and hacking should be implemented in a manner that targets malicious traffic without compromising legitimate interactions among individuals, organizations and communities. Configuring network equipment to minimize unnecessary information collection about users — given local legal and routing requirements — effectively pre-empts overbroad data requests, since companies cannot turn over information they do not have.[102] Even if user information is logged, meaningful limits on whether and for how long they are retained also restrict the scope of personal and sensitive data available for third party access.

3. Stakeholder engagement

61. Human rights engagement with governments, corporate partners and other stakeholders may prevent or mitigate human rights violations down the line. Companies that deal directly with governments should push for human rights safeguards in operating licences and sales contracts, such as assurances that network equipment will not be accessed or modified without the company's knowledge (which can be for the purpose of facilitating human rights abuses). Timely intervention during litigation (such as amicus filings in cases brought by civil society groups or peer companies against censorship or surveillance laws) and human rights-oriented lobbying in legislative and policymaking processes may also advance legal protections for freedom of expression and privacy.

62. Arrangements with corporate partners should enable all parties to uphold their human rights responsibilities. In particular, such arrangements should be designed to ensure that subsidiaries, joint venture partners, suppliers and distributors will abide by whatever freedom of expression and privacy policies the company has in place. For example, when local operations receive unconventional censorship or surveillance requests, company policy should ensure that these requests are escalated to global management for review.[103] Whistle-blowing mechanisms should be made available to both employees and contractors. To the extent that companies are already in business relationships that raise human rights concerns, they should seek to build leverage over time to prevent or mitigate harm.[104]

63. Companies may also enhance respect for human rights through collaborative action. Such collaboration includes joint outreach and advocacy with peer companies; engagement

[100] Business and Social Responsibility, "Applying the Guiding Principles on Business and Human Rights to the ICT industry", Version 2.0: Ten lessons learned, A briefing paper (September 2012), p. 9.

[101] ARTICLE 19, "Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite?" (15 September 2016).

[102] Electronic Frontier Foundation, "User privacy for ISPs and accidental ISPs".

[103] Telecommunications Industry Dialogue submission, pp. 13 and 16.

[104] SHIFT, "Using leverage in business relationships to reduce human rights risks" (New York, November 2013).

with regional or international bodies, including human rights mechanisms and economic institutions; and membership in industry associations and multi-stakeholder initiatives.[105] Regular consultations with users, civil society and affected rights holders can also mobilize public support for company efforts to resist government overreach. Cross-sector collaboration strengthens the normative force of agreed upon human rights best practices and standards, intensifying pressure on both governments and peer companies to comply.

4. Mitigation strategies[106]

64. To the extent that companies handle content regulation and user data requests, specific policies and practices to mitigate the harms of government restrictions may be adopted.

Ensure that requests for content restrictions and customer data are in strict compliance with the law

65. Companies should ensure that all requests for content restriction and customer data comply not only with procedural and legal requirements specified under local law, but also internationally established due process standards.[107] Given the intrusion on human rights, such requests should be authorized by independent and impartial courts or adjudicatory bodies. Furthermore, companies should require that requests be made in writing and present a clear explanation of the legal basis, and the name, title and signature of the authorizing official. Companies should also seek to verify that the relevant official or government entity is authorized to issue this request.[108] These formalities should be requested even if they are not required by law. Additionally, companies should preserve a written record of all communications between them and the requester relating to each request and logs of access to user data when executing the request, provided that such a record does not pose undue privacy risks.[109]

Interpreting the scope of government requests and laws

66. Vague and open-ended government requests and legal frameworks make it difficult for companies to determine whether they are in compliance with local law. However, companies can mitigate this uncertainty by adopting company-wide policies that direct all business units, including local subsidiaries, to resolve any legal ambiguity in favour of respect for freedom of expression, privacy and other human rights. Such policies are based not only on the provider's human rights responsibilities, but also the State's obligation to comply with applicable human rights laws and relevant protections under local law (such as constitutional, criminal procedure and data protection laws).

67. In practice, companies should as far as possible interpret requests in a manner that ensures the least restriction on content and access to customer data. For example, when requests appear overbroad, Global Network Initiative recommends that companies seek clarification on their scope and obtain appropriate modifications.[110]

---

[105] Telecommunications Industry Dialogue submission, p. 12; and Global Network Initiative submission, p. 7.

[106] The guidance provided in this section benefited greatly from the Telecommunications Industry Dialogue submission and the Global Network Initiative, "Implementation guidelines for the principles on freedom of expression and privacy".

[107] See, for example, the Manila Principles on Intermediary Liability and the International Principles on the Application of Human Rights to Communications Surveillance, co-authored by a number of non-governmental organizations.

[108] Global Network Initiative, "Implementation guidelines", pp. 5-6; also Telecommunications Industry Dialogue submission, pp. 8-10.

[109] Telecommunications Industry Dialogue submission, pp. 8-9.

[110] Ibid.

Challenge requests and underlying laws

68. Companies have an interest in operating in a legal environment that is human rights compliant, consistent due process and rule of law norms. Companies should explore all legal options for challenging requests that are excessively intrusive — such as requests for shutdowns of entire services or platforms, website takedowns that are clearly targeted at criticism or dissent or customer data requests that cover broadly unspecified users.[111]

69. Like any decision to bring legal proceedings, companies may take into account a range of considerations, such as the "potential beneficial [human rights] impact, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend".[112] However, companies should assign substantial overall weight to human rights considerations in their decision-making processes and carefully assess both the potential benefits and risks to human rights. For example, companies should be inclined to challenge overbroad requests where there is a reasonable likelihood of success, even if these challenges might be resource intensive; on the other hand, companies might pursue alternative options if a challenge is likely to create adverse precedent or backlash and undermine expression and privacy.

5. Transparency

70. Transparency is a key feature of the digital access industry's responsibility to respect. Information about government activities that require corporate assistance or involvement should be disclosed to the maximum extent allowed by law. Companies should be mindful that such information is primarily used by civil society to challenge human rights abuses in court, register grievances before domestic or international mechanisms on behalf of users or seek alternative means of accountability. Accordingly, such disclosures should be regular and ongoing, and in an accessible format that provides appropriate context.

71. Even if local law limits full transparency, companies should nonetheless disclose all relevant and publishable information. For example, if companies are prohibited from disclosing the origin or basis of a shutdown request, they should nevertheless seek to provide regular updates about the services affected or restored, the steps they are taking to address the issue and explanations after the fact. Innovative transparency measures, such as the publication of aggregate data and the selective withholding of information,[113] also mitigate the impact of gag orders and other non-disclosure laws. Companies should disclose all the local laws with which they comply and, where possible, challenge any law or regulation that prevents or hinders them from being transparent to users and the general public.[114]

72. Companies should disclose their policies and actions that implicate freedom of expression. Relevant disclosures include data retention and use policies, network management practices and the sale and purchase of network filtering and interception technologies.[115] Companies should also disclose information about the frequency, scope and subject matter of due diligence processes and a summary of high-level findings. In general, companies should consult the growing number of resources that study valuable transparency indicators and other transparency best practices. Users, civil society and peer companies should also be consulted on the design and implementation of transparency measures.

[111] Yael Ronen, "Big Brother's little helpers" (February 2015), p. 81.

[112] Global Network Initiative, "Implementation guidelines".

[113] For example, when "Telia Company was required to suspend services, the company did not state that this was the result of technical problems", Telecommunications Industry Dialogue submission, p. 14.

[114] Telecommunications Industry Dialogue, "Information on country legal frameworks pertaining to freedom of expression and privacy in telecommunications" (2016).

[115] Ranking Digital Rights submission.

6. Effective remedies

73. While certain aspects of corporate responsibility have advanced in recent years, remedial steps often seem omitted from the private sector's agenda. Yet remedies are a key pillar of corporate responsibility and should be provided whenever businesses "have caused or contributed to adverse impacts" (see A/HRC/17/31, annex, principle 22). States bear the primary duty to remediate business-related human rights abuses, particularly those they instigate, such as overbroad content restriction, unlawful user data requests and disproportionate surveillance. Yet companies that fail to implement appropriate due diligence measures and other safeguards may also cause or contribute to such abuses. In those situations, companies should "provide for or cooperate in their remediation through legitimate processes" (Ibid.).

74. Remedies may include both financial and non-financial means (Ibid., principle 27). When freedom of expression is impaired, appropriate remedies may include access to grievance mechanisms and information about the violation and guarantees of non-repetition.[116] Users whose accounts have been wrongly suspended may want the satisfaction of being heard and provided with explanations and assurances of non-repetition.[117]

75. Pre-existing policies and mechanisms could also be reformed or strengthened to address violations of freedom of expression. For example, a provider could make improvements to its content restriction policy and the training of its content moderation teams to reduce the likelihood of unfair website takedowns or overbroad content restrictions such as filtering. Customer complaint mechanisms could also be updated to allow users to flag network traffic management practices, commercial filtering classifications and other content restrictions they deem to be unduly restrictive or unfair.

V. Conclusions and recommendations

76. **Individuals depend on digital access to exercise fundamental rights, including freedom of opinion and expression, the right to life and a range of economic, social and cultural rights. They also regularly face obstacles to access: from shutdowns to surveillance. The present report is largely concerned with the obstacles that deny, deter or exclude expression through blunt reliance on digital censorship. The present report has not addressed other serious obstacles — such as the lack of adequate connectivity infrastructure, high costs of access imposed by government, gender inequality, and language barriers — that also may constitute forms of censorship.**[118] **Much of it therefore focuses on the roles and obligations of States. But States increasingly exercise censorship through the private sector. The report has aimed not only to address the constraints on State action under human rights law but also the principles that private actors should observe in respecting human rights. Key recommendations, already highlighted in the analysis above, are set out below.**

States and the Human Rights Council

77. **The Human Rights Council, in its resolution 32/13, condemned unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and called upon all States to refrain from and cease such measures. This condemnation, which is critical to the Council's promotion of human rights online, should be supplemented and specified. Intentional prevention or disruption of access includes any action that shuts down or**

[116] Telecommunications Industry Dialogue submission, p. 17.

[117] Peter Micek and Jeff Landale, "Forgotten pillar: the Telco remedy plan", Access Now (May 2013), p. 6.

[118] Global Commission on Internet Governance submission; Arco Iris Libre de Cuba, Centro de Información Hablemos Press, Centro de Información Legal CubaLex, Mesa de Diálogo de la Juventud Cubana Plataforma Femenina Nuevo País, "Situación del derecho a la libertad de opinion y expression en Cuba" (Situation of the right to freedom of opinion and expression in Cuba) (July 2016), p. 20.

renders ineffective access to telecommunications networks, mobile services, social media platforms and so forth. Future work of the Council that clarifies the rules that apply to digital access, as outlined in this report, would advance the right to freedom of opinion and expression online.

78. **It is also critical for the Council and States to draw the connections between privacy interference and freedom of expression. To be sure, interferences with privacy must be assessed on their own merits under article 17 of the International Covenant on Civil and Political Rights and other norms of human rights law. But certain interferences — such as overbroad requests for user data and third party retention of such data — can have both near- and long-term deterrent effects on expression, and should be avoided as a matter of law and policy. At a minimum, States should ensure that surveillance is authorized by an independent, impartial and competent judicial authority certifying that the request is necessary and proportionate to protect a legitimate aim.**

79. **The Special Rapporteur is particularly concerned about reports of threats and intimidation of companies, their employees and their equipment and infrastructure. Also, the Council's emphasis on the important role — and need for protection — of the private sector deserves consideration. States should review all activities to obtain network access to ensure that they are lawful, necessary and proportionate, paying particular attention to whether these activities are the least intrusive means for protecting a legitimate aim.**

80. **The protective role that States may exercise over the private sector can only go so far. They should not be promoting the economic gain of private entities over users' rights to freedom of opinion and expression. Thus, States should prohibit attempts to assign priority to certain types of Internet content or applications over others for payment or other commercial benefits.**

81. **The intersection of State behaviour and corporate roles in the digital age remains somewhat new for many States. One profitable way forward, at both the international and domestic levels, would involve the development of national action plans on business and human rights in order to establish meaningful avenues for all categories of the digital access industry to identify and address their respective human rights impacts.**

Private actors

82. **For years now, individuals and companies within the digital access sector have understood that they play an essential role in the vast expansion of access to information and communications services. They are in a business in which the model for success should involve expanding access, efficiencies, diversity and transparency. They should take the principles identified in the present report as tools to strengthen their own roles in advancing users' rights to freedom of expression. In this spirit, in addition to high-level policy commitments to human rights, the industry should allocate appropriate resources towards the fulfilment of these commitments, including due diligence, rights-oriented design and engineering choices, stakeholder engagement, strategies to prevent or mitigate human rights risks, transparency and effective remedies. In doing so, the design and implementation of corporate human rights accountability measures should draw on both internal and external expertise, and ensure meaningful input from customers and other affected rights holders, civil society and the human rights community.**

83. **This is not to say that private companies do not face pressures. They do. But when States request corporate involvement in censorship or surveillance, companies should seek to prevent or mitigate the adverse human rights impacts of their involvement to the maximum extent allowed by law. In any event, companies should take all necessary and lawful measures to ensure that they do not cause, contribute or become complicit in human rights abuses. Arrangements with corporate partners should be structured to ensure that all parties uphold their human rights**

responsibilities. Companies should also seek to build leverage in pre-existing business relationships to prevent or mitigate adverse human rights impacts.