their implementation of the United Nations Guiding Principles for Business and Human Rights.

28 In this vein, the Human Rights Protocol Considerations Research Group of the Internet Research Task Force – an IETF affiliate that focuses on longer-term research issues – is developing guidance to facilitate "conscious and explicit design decisions" that take into account human rights considerations.[63] In particular, this guidance poses a series of questions on issues ranging from privacy to content agnosticism and internationalization that developers can take into account at "any point in the design process". [64] This methodology is similar to Human Rights Impact Assessments that several Internet and telecommunications companies conduct during the design and engineering phase of product development.

29. Policies and practices that facilitate a more transparent and inclusive protocol design process should also be encouraged. Meaningful access to information concerning "the development of a standard and associated deliberations, minutes, and records" provides opportunities for public input, establishing public accountability and oversight.[65] Increasing the participation of engineers with human rights expertise and civil society representatives will also empower SDOs to better identify and address the human rights impact of their work.[66]

III. Overview of Submissions Received in Preparation of A/HRC/35/22

30. The Special Rapporteur's call for input generated 25 submissions from States; 3 from companies; 22 from civil society, academics and others; and 1 confidential submission. The Special Rapporteur is extremely grateful for the submissions received, each of which informed, in one way or another, the report itself. The submissions referenced in this report may be found at the website of the mandate.

A. The Provision of Internet and Telecommunications Access: Freedom of Expression Issues and Concerns

i. Internet and Telecommunications Shutdowns

31. Various submissions discussed the scale, duration, and frequency of shutdowns, as well as the types of services affected. See Bahrain Center for Human Rights at 13, Access Now ("Access") Part I at 12, and Internet Sans Frontieres ("ISF") at 1. Access's submission also provides an overview of various domestic legal frameworks concerning the authority to order shutdowns. See Access Analysis of Shutdown Laws.

32. One submission discussed the technical means used to shut down networks or otherwise censor the Internet. In particular, network disconnection or adversarial route announcement, which "withdraws all of the Boarder (sic) Gateway Protocol (BGP) prefixes routing through the censor's country", is "perhaps the crudest of all censorship techniques" and has the effect of "shutting off the network". See Center for Democracy and Technology ("CDT") Part III at 16.

---

[63] Human Rights Protocol Considerations Research Group, https://irtf.org/hrpc.

[64] Content agnosticism is defined as the treatment of "network traffic identically regardless of content." draft-irtf-hrpc-research-13 at 43. Internationalization is defined as the "practice of making protocols, standards, and implementations usable in different languages and scripts." *Id*. At 44.

[65] DeNardis at 84.

[66] Cath & Floridi at 465.

33. Submissions highlighted common government justifications for shutdowns, and their incompatibility with international law. See ISF at 2, and Access Part I at 5.

34. Submissions also discussed the impacts of shutdowns, including their impact on the exercise of human rights other than freedom of expression, democratic and political participation, and the economy. See Access Part I at 2, Global Network Initiative ("GNI") at 4, and Telecommunications Industry Dialogue ("TID") at 2.

35. One submission proposed restricting the authority to conduct shutdowns through an amendment to the Constitution of the International Telecommunications Union. See Association for Proper Internet Governance.

36. Various submissions addressed the need for multi-stakeholder collaboration to address shutdowns. See GNI, Access Part I at 15-16.

ii. Other Forms of Content Blocking and Regulation

37. Although the report focuses on shutdowns, submissions discussed a wide variety of forms of online censorship.

38. Certain forms of censorship are directly conducted by States, which often grant government agencies broad authority to block or restrict access to a wide range of online content. See ARTICLE 19 submission at 2. For example, the National Authority for Management and Regulation in Communications of Romania ("ANCOM") has the authority to require ISPs to block certain "pornographic content, illegal gambling, or products likely to have psychoactive effects". See Romania at 1. Estonia's Gambling Act requires ISPs to "block access to online casinos which do not pay gambling taxes to Estonia". See Estonia at 1. In China, the government "deploys sophisticated technology, including the "Great Firewall", to monitor online communications, conduct surveillance, and block undesirable content". See Human Rights in China ("HRIC") at 1. China also "enlists voluntary company initiatives and the online community in monitoring and censoring expression". *Id*. at 28-30.

39. Other forms of censorship are conducted by private actors at the direction of States. Content blocking obligations are frequently "included directly in licensing obligations", requiring Telcos and ISPs to "block or filter certain types of content, such as pornography or otherwise contrary to "good morals". See ARTICLE 19 at 3. Telcos "can block access to entire websites, specific pages or specific keywords"; such blocking "prevents users from receiving information but can also prevent users from posting information to a specific location such as in the case of social networks". See Ranking Digital Rights ("RDR") at 9.

40. Several States mandate that ISPs must offer filtering services to their customers. Under Section 41 of Israel's Communications Law (Bezeq and Broadcasting) 5742-1982, ISPs are obliged to "notify subscribers regarding offensive websites and offensive content [as defined in the law], and the possibilities of protection against them, including technological means which are intended to filter such websites or content". See Israel at 2-3.

41. Copyright enforcement is another area of content regulation that raises significant concerns for freedom of expression. One submission notes that "copyright owners are increasingly seeking to enlist the assistance of [ISPs] to enforce copyright and impose sanctions on their users". See Nicolas Suzor ("Suzor") at 3. In Europe, the European Commission is reportedly "putting pressure on companies to "voluntarily" impose sanctions on online services accused of infringements". See European Digital Rights ("EDRi") at 3-4. For criticisms of Australia's copyright regime, see Digital Rights Watch ("DRW") at Section 2.

42. Various submissions discussed the human rights impact of content regulation on social media and other Internet platforms. See ADF International; Suzor. While these issues

are beyond the scope of the present report, the Special Rapporteur plans to address them in future reporting.

43. For an analysis of common network censorship techniques, including HTTP Request Header Identification, Deep Packet Inspection ("DPI") Identification, and TCP/IP Header Identification, see CDT Part III.

44. The Special Rapporteur has previously outlined the range of content regulation issues that implicate both States and the private sector (A/HRC/32/38 at para.10-12).

iii. Net Neutrality

45. Submissions discussed various forms of interference with net neutrality, and their impact on freedom of expression. For an overview of the "wide array of [network] traffic management practices [employed by Telcos and ISPs] resulting in undue restrictions", see Luca Belli ("Belli") at 3-4.

46. The benefits of zero rating and the risks they pose to freedom of expression are the subject of much debate, and depend to some extent on the type of zero rating arrangements at issue. Arrangements that offer unmetered access to certain applications, content or services without the purchase of a data plan (such as "Free Basics") are particularly contentious. Supporters argue that these arrangements facilitate freedom of expression by providing some degree of Internet access to areas that would otherwise lack connectivity. As more users go online with the assistance of these arrangements, the theory goes, the price of connectivity will be lowered, broadband infrastructure will improve, and digital innovation will increase. See CDT Part I (A) at 11. But these outcomes are far from guaranteed, and highly dependent on factors such as user behavior, market conditions and the regulatory environment. Users conditioned to rely on zero rated platforms might be reluctant to seek out new content and services. Well-established platforms might also be able to secure better terms of access to zero rating arrangements than smaller competitors, reinforcing their dominance and their impact on user choice. Finally, the continued presence of zero rating in an emerging market could incentivize low data caps and inflate the price of metered data, even as Internet adoption increases. At the very least, whether and how zero rating might lead to Internet adoption while minimizing the risk of creating permanently walled online gardens is in need for further study. See CDT Part I (A) at 15. See also Access Part II at 18-19; Fundacion Karisma at 6-7.

47. Various States discussed domestic efforts to regulate and protect net neutrality in their submissions. Estonia and Slovakia stated that they had implemented relevant European Union net neutrality regulations in their domestic law. Bulgaria stated that net neutrality regulation should be "directed towards finding a balance between preserving the open character of the Internet and guaranteeing the fundamental rights of consumer", and that on certain aspects of net neutrality (such as quality of service issues and anti-competitive blocking), "there should be an opportunity for intervention of a competent authority". See Bulgaria at 5. Norway stated that its guidelines on net neutrality seek to ensure that the Internet remains "an open and non-discriminatory platform for all types of communication and content distribution". See Norway at 5. EDRi's submission also highlighted the Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, adopted by the Body of European Regulators ("BEREC").

48. Telefonica was the only company that provided input on the issue of net neutrality. Telefonica's position is that it understands the need for the "protection of users' rights and their freedom of user choice", but at the same time claims "the ability to manage traffic on our networks, and permit differentiation of Internet access service". See Telefonica at 1-2.

49. One submission highlighted the Model Framework on Network Neutrality developed by the Dynamic Coalition on Network Neutrality, a multi-stakeholder initiative of the UN Internet Governance Forum. See Belli.

iv. Government Access to User Data

50. Concerns regarding government access to user data held by the private sector were a persistent theme throughout the submissions. See, e.g., EDRi (discussing provision or facilitation of access to consumer data in the EU); CDT Part I (B) (outlining a descriptive framework and a normative framework for analysing and comparing domestic laws on surveillance and government access to user data); RDR (analyzing telecommunications companies' disclosures to users about how their information is handled); DRW (discussing remedies for undue access to customer data).

51. Various submissions raised human rights concerns arising from direct access to Internet and telecommunications networks – a practice that is still shrouded in secrecy. See Privacy International ("PI"); TID at 3; CDT Part I (B) at 30; Fundacion Karisma at 1 (discussing Colombia's law requiring installation of networks that enable government access).

52. Many submissions discussed data retention requirements imposed by governments on private actors, and the privacy concerns these create. See submissions of CDT Part I (B) at 31; Access Part II (analysing data retention in Latin America and the EU); Fundacion Karisma at 2 (discussing Colombia's data retention and mobile registration requirements); Bahrain Center for Human Rights at 17 (discussing Bahrain's data retention requirements); DRW at Section 1 (discussing Australia's data retention regime); HRIC at 12 (discussing data localization and real name identification laws in China).

53. States' submissions illustrate the range of legislative and regulatory frameworks that authorize government access to customer data. States that provided information concerning relevant laws and regulations include: Bulgaria (Article 304 of the Electronic Communications Act); Canada (Section 37 of the Telecommunications Act); Estonia (Section 111 and 113 of the Electronic Communications Act); Finland (Section 185 of the Information Society Code); Georgia (Article 8(1) of the Law of Georgia on Electronic Communications); Japan (Telecommunication Business Act); the Philippines (Anti-Wiretapping Law, Cybercrime Prevention Act)), Serbia (Section 17 of the Law on Electronic Communications); and Slovakia (Part 4 of the Electronic Communications Act, titled Protection of Privacy and Personal Data). Notably, Canada and Japan require judicial pre-authorization for certain forms of government access.

54. Submissions also raised concerns about the lack of government transparency concerning their access to user data. See, for example, CDT Part I (B) at 15 (discussing vague and ambiguous laws, opaque surveillance practices, inadequate oversight and reporting mechanisms, and the lack of transparency concerning voluntary data sharing); Access Part II at 15-16 (discussing government non-compliance with transparency obligations under their own domestic laws); PI (discussing general lack of transparency concerning direct access); and GNI at 3-4 (observing that "many governments' legal frameworks continue to prohibit publication of [information about government requests for user data] by companies").

55. On the other hand, a few governments have established transparency measures that appear to be a step in the right direction. For example, Canada adopted "Non-binding Transparency Reporting Guidelines" that aim to help "private organisations [be] open with their customers regarding the management and sharing of their personal information with government entities such as law enforcement and national security agencies". See Canada at 8. In Finland, under the Act on the Openness of Government Activities (621/1999), "all official documents are in the public domain, unless their publication has been specifically restricted". See Finland at 6.

56. Human Rights concerns associated with government access to user data have been addressed in the Special Rapporteur's previous reports. In particular, the Special Rapporteur has previously analyzed threats to encryption and anonymity (A/HRC/29/32),

and the human rights impact of communications surveillance (A/HRC/23/40). The UN Office of the High Commissioner for Human Rights has also analyzed the protection and promotion of the right to privacy in the context of domestic and extraterritorial communications surveillance (A/HRC/27/37).

v. Digital Inclusion and Accessibility Concerns

57. A few submissions also addressed the continued lack of Internet access in many parts of the world. In Latin America, for example, one submission observed the need to "complement infrastructure-deployment initiatives and regulatory reforms with targeted programs aimed at addressing connectivity barriers", such as "incentives for the creation of online content and services in indigenous languages", kindergarten to grade 12 school connectivity initiatives, and residential access subsidies for low-income families. See Global Commission on Internet Governance at 1. In Australia, one submission observed that the "significant digital divide" in the country has a particularly detrimental impact on "older Australians, indigenous people and people with disabilities, among others". See DRW at Section 6. It also argued that "competition and consumer laws are … important to closing the digital divide". *Id*.

B. The Human Rights Responsibilities of the Digital Access Sector

i. Developments in Multi-Stakeholder Governance

58. On 27 March 2017, the Global Network Initiative ("GNI") expanded its membership to include six Telcos/ISPs and one network equipment vendor. The seven new members were formerly members of the Telecommunications Industry Dialogue ("TID"). When they joined the GNI, the TID ceased to be a functioning entity. The full list of GNI members may be found on its website.

59. Since the publication of the Special Rapporteur's main report (A/HRC/35/22), the GNI has also updated its Principles on Freedom of Expression and Privacy ("Updated GNI Principles"), as well as the accompanying Implementation Guidelines ("Updated GNI Guidelines"). These documents may be found on its website. Although there is significant overlap between the updated versions and the versions relied on in the main report, there are notable differences, some of which are noted below.

ii. Due Diligence

60. TID's submission discusses how member companies conduct Human Rights Impact Assessments ("HRIA") and other due diligence measures. TID at 7-8. GNI's submission discusses its Independent Company Assessment process, a "review of relevant internal systems, policies and procedures for implementing the GNI principles". See GNI at 8.

61. In separate submissions, Telefonica and Yahoo! explain their respective HRIA and due diligence processes in greater detail.

62. The Updated GNI Guidelines appear to contemplate a range of due diligence processes and mechanisms other than HRIAs. See Guidelines 2.4-2.7. Examples of business activities that should trigger due diligence are also identified. See Guideline 2.6.

63. The submissions identified several examples of HRIAs and due diligence measures.

64. In 2012, Telefonica, with the support of Business for Social Responsibility ("BSR"), conducted an HRIA "of all our operations to assess the global impact of our activitiy". Telefonica is continuing to integrate the results of the HRIA across its business operations. In 2015, Telefonica implemented "[p]eriodical reviews of the most significant risks in matters of privacy and security which affect our business at a global level". See Telefonica at 5.

65. In 2014, Orange "worked with Maplecroft to implement a customized risk index encompassing the 30 countries in which it is present as a mass-market operator". See TID at 7.

66. From 2015 to 2016, Telia Company, with BSR's support, conducted an HRIA of its plans to divest its Region Eurasia businesses. See TID at 7.

67. Nokia uses a "human rights due diligence process" to "identify potential risks for product misuse and to investigate ways to mitigate these risks". Flagging of potential risk cases is "embedded in the company's sales tool as an automated feature, thus minimizing the risk of missing any cases due to human error". See TID at 7.

68. Yahoo conducts "short-form" HRIAs for "specific, targeted questions" and "long-form" HRIAs when it "identifies significant risks to users' free expression and/or privacy". See Yahoo at 6-7.

69. HRIAs may lead to significant changes in a company's business plans and product or service design. For example, Yahoo's HRIA on its entry into Vietnam led the company to "manage and operate out Vietnamese language services out of Singapore so the services would be governed by laws with stronger protections than those in Vietnam". See Yahoo at 7.

iii. Stakeholder Engagement

70. Various submissions discussed ongoing and potential efforts to address threats to freedom of expression through collective action and multi-stakeholder collaboration. See, for example, PI (urging collective action to "bring transparency to [direct access] and begin to raise standards within a country and set best practice"); TID at 0-1 (discussing TID's efforts to "make available guidance and information on the main laws, regulations and standards that are applicable to licensed operators"); and GNI (discussing collaboration to address network shutdowns).

iv. Mitigation Strategies

71. The submissions identified examples of company policies and practices developed to handle government requests for content restriction and user data.

72. AT&T trains relevant employees to "confirm that requests are duly issued by an appropriate entity, under valid legal authority and … otherwise in compliance with applicable requirements". The review process may include AT&T lawyers and where necessary, local counsel familiar with applicable law. See TID at 8.

73. Millicom finalized its "Guideline for Law Enforcement Assistance Requests" in 2015, which establishes procedures for handling, among other things, "urgent and non-written requests, how to log requests and our responses, how to protect customer data through the process of retrieving information, and how to deliver the information safely". See TID at 8-9.

74. The submissions also identified company strategies to mitigate or minimize the potential human rights impact or unlawful government demands or action.

75. In the past, Millicom and Orange have insisted on written government requests that comply with all necessary formatting and procedural requirements. See TID at 9.

76. Orange is also "setting up an emergency procedure" that sends an alert to the GNI, NGOs and other relevant stakeholders when it receives an unlawful or otherwise "unacceptable" government request. See Orange at 1.

77. Telenor "engages actively with relevant authorities", seeks clarifications on problematic requests, and, when needed, engages "diplomatic channels and international

organizations". Telenor also raises the need to "engage in longer-term dialogue, and not only when an incident occurs". See TID at 10.

78. When dealing with government requests, both TID and GNI emphasize the need to "[a]lways seek to ensure the safety and liberty of company personnel who may be placed at risk". See TID at 10-11; Updated GNI Principles, Principle 4 on Responsible Company Decision making.

v. Transparency

79. Various submissions highlighted areas where greater corporate transparency should be encouraged.

80. RDR, a "project to benchmark the world's largest internet, telecommunications, and other ICT companies" on their policies and practices affecting freedom of expression and privacy, identified several areas where greater corporate transparency is required. On network shutdowns, RDR found that less than half of the Telcos and ISPs it examined disclosed whether they notified users of access restrictions, and even fewer provided information about their process for responding to shut down requests. See RDR at 7- 8. RDR also urged companies to provide meaningful information concerning the "blocking and filtering practices of internet access services" they operate, as well as their network traffic management practices. See RDR at 9 - 10. Additionally, RDR found "industry-wide incoherence in disclosures to users about how companies handle their information," including "what is collected, how it is collect, how long it is retained, and with whom it is shared". See RDR at 11 - 12.

81. PI's submission contains specific recommendations on how companies can collectively seek to bring transparency to the "highly secretive process" of direct access.

82. GNI observed "despite increasing numbers of Telcos and ISPs adopting the practice of releasing transparency reports with information about government requests for user data, many governments' legal frameworks continue to prohibit publication of such data by companies". See GNI at 3.

83. Several Telcos and ISPs provided information on their transparency policies and practices. For example, Telenor stated that transparency "is not always easy, and in some instances, may have unintended and negative effects on efforts to minimize the impact on privacy and freedom of expression"; nevertheless, its stance "is to be transparent and this is communicated to the relevant authorities". See TID at 10. Telia Company has "made publicly available its internal tool for assessments and escalation of government requests and demands with potentially serious impacts on freedom of expression in communications", and has also begun to "report publicly on unconventional requests and demands with potentially serious impacts on the right to freedom of expression". See TID at 12, 14.

vi. Effective Remedies

84. Under the Updated GNI Guidelines, member companies are required to develop grievance mechanisms for users to raise "grievances about issues related to freedom of expression and privacy to be communicated to the company for consideration". Additionally, if a member company "determines its business practices are inconsistent with the [Updated GNI] Principles or have caused or contributed to adverse impacts, it will establish by itself or in cooperation with other actors, a means of remediation, including meaningful steps to prevent recurrence of such inconsistency or impact". See Guideline 2.13 (f).

85. RDR evaluates the effectiveness of a company's grievance and remedy mechanisms based on whether the company: (i) discloses its processes for receiving complaints or grievances, (ii) lists the kinds of complaints it is prepared to respond to, (iii) articulates its

process for responding to complaints, (iv) reports on the number of complaints received, and (v) provides evidence that it is responding to complaints, including examples of outcomes. See RDR at 6.

86. Access Now has developed a Telco Remedy Plan that provides guidance on the implementation of "the procedural aspects of remedy, such as safe and accessible grievance mechanisms, and the substantive aspects, which may be as simple as an explanation and commitment to non-repetition". Access Part II at 23.

87. The State potentially plays a critical role in ensuring access to effective remedies for violations of freedom of expression and privacy. In Australia, the Privacy Principles establish "a complaint process for individuals who believe they have had their privacy breached". Complaints are assessed by the Information Commissioner, and may result in civil penalties. See DRW at Section 5. Bharti Airtel, a Telco in India, scored the highest on RDR's survey of corporate grievance and remedy mechanisms, "due primarily to India's regulatory requirements in relation to remedy". See RDR at 6.

vii. Other Private Actors

88. One submission noted that, in the context of direct access, "there are other companies in the ICT ecosystem where [their] role … [is] less clear" and "needs to be explored". In particular, network equipment vendors, Internet Exchange Points, and submarine cable providers are among the companies that require further scrutiny. The role of Internet companies in establishing and managing undersea cables is also relevant. See PI at 8-9.

IV. Summary of Multi-Stakeholder Consultation on Human Rights Due Diligence and the Digital Access Industry

89. The Special Rapporteur co-organized and participated in four meetings that helped inform the main report: (1) an informal brainstorming session hosted by ARTICLE 19 in London on 22 July 2016; (2) an experts meeting hosted by the University of Connecticut on 24 October 2016; (3) a regional consultation with the Special Rapporteur on Freedom of Expression for the Inter-American Commission on Human Rights, hosted during the Internet Governance Forum in Guadalajara on 5 December 2016; and (4) a regional meeting in Beirut, hosted by the Special Rapporteur on 29 February - 1 March 2017, that touched in part on the issues in the report. The Special Rapporteur also conducted a special preview of the report hosted during RightsCon in Brussels on 30 March 2017.

90. This section summarizes the 24 October 2016 consultation hosted by the University of Connecticut. This consultation focused specifically on understanding the nature and scope of a company's obligation to engage in due diligence to assess human rights impacts in the Internet and telecommunications access industry. The private actors at issue included Telecommunications Providers ("Telcos"), Internet Service Providers ("ISPs"), Network Equipment Vendors ("Vendors"), Internet Exchange Points ("IXPs"), and Submarine Cable Providers.

91. The consultation was organized around four themes: Identifying Human Rights Risks, Due Diligence Practices and Procedures, Remedies, and Transparency. The discussion was held under modified Chatham House Rules: While participants are listed below, comments are not attributed to particular speakers or participants, nor are the opinions and interventions noted in this summary intended to suggest shared agreement on those points among the participants.

92. Seventeen participants (excluding the Special Rapporteur and his team) attended the consultation (affiliations listed here for identification purposes only): Barbora Bukovská (ARTICLE 19), Camilla Goldbeck-Löwe (Ericsson), Leslie Harris (Harris Strategy Group),