United Nations

A/HRC/35/22/Add.4

General Assembly

Distr.: General
22 May 2017

English only

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 protection and promotion of the right to freedom of opinion and expression

Addendum

Supplementary Materials Accompanying Annual Report A/HRC/35/22*

* The present document is being circulated in English only, as it exceeds the word limitations currently imposed by the relevant General Assembly resolutions.

Contents

I. Introduction

1. This annex accompanies the June 2017 report to the Human Rights Council of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression (A/HRC/35/22). The main report examines the role of State and non-State actors in the provision of Internet and telecommunications access (or "digital access") and their human rights obligations and responsibilities respectively. The report provides guidance concerning the responsibility of digital access providers to respect freedom of expression online.

2. Part II of the Annex discusses the **human rights impact of Standards Developing Organization ("SDOs").** The report explains that SDOs, while not strictly "industry actors", nevertheless "establish technical protocols and standards that enable inter-operability in the telecommunications and Internet infrastructure" (A/HRC/35/22). Part II thus explores the work and governance of major SDOs, their impact on freedom of expression, and the need to incorporate human rights due diligence into standards development.

3. Part III provides an overview of **the submissions that the Special Rapporteur received** from States, civil society organizations, companies, academics and others. Given space limitations, the main report could not discuss these submissions in detail. Part III thus highlights issues and concerns raised in these submissions and other resources that interested readers may wish to investigate.

4. Part IV provides a summary of a **multi-stakeholder consultation on human rights due diligence and the digital access industry** conducted in preparation of the report. The consultation was held on 24 October 2016 and hosted by the University of Connecticut, one of several meetings that helped inform the report.

5. The Special Rapporteur would like to thank the following for their invaluable assistance in preparing this annex: Calvin Bryne, Sarah Choi, and Adam Lhedmat of the International Justice Clinic at the University of California ("UC"), Irvine, who helped research and draft Parts II and III; Molly Land, Fatimah Belem, Katharina Braun, Dorothy Diaz-Hennessey, Richard Hine, and Komla Matrevi of the University of Connecticut, and Katherine Ells of UC Irvine, who helped compile Part IV; and Amos Toh, who coordinated and edited the annex.

6. This annex should be read as a companion to A/HRC/35/22 and does not intend to endorse or reject any of the input provided during the preparation of the report.

II. On the Human Rights Impact of Standards Developing Organizations

7. The Special Rapporteur has identified the development of technical standards as a critical area of human rights discourse (A/HRC/35/22; paras. 43-44; A/HRC/32/38, paras. 27-29). The capacity to seek, receive and impart information online relies on an ever-expanding series of standards and protocols that enable the smooth functioning of Internet and telecommunications networks. The TCP/IP protocols, for example, determine how information should be formatted, addressed and routed among devices within a network and between networks.[1]

[1] See "Transmission Control Protocol/Internet Protocol (TCP/IP)," Techopedia *available at* https://www.techopedia.com/definition/2460/transmission-control-protocolinternet-protocol-tcpip;

A. Standards Developing Organizations

8. Internet and telecommunications standards are developed by a wide variety of Standards Developing Organizations ("SDOs"). Some of these SDOs are loosely governed, composed of volunteers and open to anyone to join, while others have more formal membership structures with varying levels of participation. Many of them attract significant participation from the private sector, while academic and other civil society participation is also common. Major SDOs include:

i. Internet Engineering Task Force ("IETF")

9. *What they do:* Most commonly known for its role in developing the first iteration of the Internet, IETF's primary mission is to develop Internet standards. In particular, it "[p]lays a crucial role in managing the logical layer of the Internet, and in designing the standards and protocols that define how information flows across the networks."[2]

10. *Governance:* IETF has no official membership, and its activities are open to anyone.[3] However, many of those involved in drafting standards and the organization's governance are affiliated with the private sector.[4] IETF is organized into seven areas of work: Applications and Real-Time Area (focused on Internet applications protocols and architectures), Internet Area (IP layer protocols), Operations and Management Area (network management), Security Area (security protocols), Routing Area (protocols ensuring continuous operation of the Internet routing system), Transport Area (data transport protocols), and General Area (supporting, updating and maintaining the standards development process).[5] Each Area is managed by one or two Area Directors, who ensure that the "Area is well coordinated, that there is coverage for the technologies needed in the area, and that the challenges most important to the Internet in that area are indeed being worked on."[6] Within each Area, IETF standards are mainly developed through Working Groups ("WGs") and published in documents known as Requests for Comments ("RFCs").[7] Anyone may set up a WG, provided that the advice and consent of the relevant Area Director is obtained and the WG complies with the guidelines and procedures for its formation and operation.[8] Standards are adopted through a consensus-building process that seeks to reflect the "dominant view" of the WG in the event that unanimity cannot be achieved (referred to in the IETF as "rough consensus").[9] WG decisions are frequently made via e-mail on publicly available mailing lists.[10] IETF's three annual meetings also provide an opportunity for WGs to meet and make decisions, and for the organization as a

See also DeNardis, Laura, *The Global War for Internet Governance*, Yale University Press (2014) at 67.

[2] ARTICLE 19 submission at 12.

[3] See Internet Society submission at 5; Internet Engineering Task Force, "Getting Started in the IETF" *available at* https://www.ietf.org/newcomers.html.

[4] DeNardis at 66-67, 70.

[5] IETF, "Areas," *available at* https://www.ietf.org/iesg/area.html.

[6] *Id*.

[7] S. Bradner (ed.), Network Working Group, IETF, "IETF Working Group Guidelines and Procedures," RFC 2418 (September 1998), 4, 20, *available at* https://tools.ietf.org/html/rfc2418#. The list of active IETF WGs is *available at* https://datatracker.ietf.org/wg/.

[8] RFC 2418 at 4-9.

[9] IETF participants have stressed that "rough consensus" is not majoritarian rule - "51% of the working group does not qualify as "rough consensus" and 99% is better than rough." Consensus is determined not on the "basis of volume or persistence, but rather a more general sense of agreement." RFC 2418 at 13. See also P. Resnick, IETF, "On Consensus and Humming in the IETF," RFC 7282 (June 2014), *available at* https://tools.ietf.org/html/rfc7282 (discussing and critiquing the features of "rough consensus").

[10] ARTICLE 19 submission at 12.

whole to discuss key technical and administrative issues concerning its role in setting Internet standards.[11] During these meetings, consensus is usually determined by humming.[12]

ii. World Wide Web Consortium ("W3C")

11. *What they do:* Another large and well-established SDO, W3C is a membership organization that develops standards and protocols for the World Wide Web, one of the most widely used Internet applications for communication and information exchange (and often synonymous with the Internet for most users).[13] W3C standards include the HyperText Markup Language ("HTML") and Extensible Markup Language ("XML"), the main language responsible for websites. At the time of publication, W3C is considering the adoption of the Encrypted Media Extensions ("EME") specification, which would accommodate the use of Digital Rights Management ("DRM") (software that restricts access to proprietary or copyrighted works) on web browsers.[14] The proposed specification has raised concerns that it will become easier for large media companies to impose onerous restrictions on access to digital content.[15]

12. *Governance:* W3C membership is open to companies, universities, governmental organizations, non-profit entities, and individuals.[16] However, the majority of the active members work for companies whose products employ web standards.[17] W3C is funded by its membership, based on a sliding scale adjusted for factors such as the location in the world and the type of entity.[18] Standards are adopted based on consensus through technical discussion and compromise among relevant members.[19] When there is a deadlock and all available means of consensus have been exhausted, a formal vote is conducted.[20]

iii. International Telecommunication Union's Telecommunication Standardization Sector ("ITU-T")

13. *What they do:* ITU-T is one of three sectors that comprise the International Telecommunications Union, a specialized UN agency dedicated to the development of

[11] Paul Hoffman (ed.), IETF, "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force," available at https://www.ietf.org/tao.html.

[12] RFC 2418 at 13; ARTICLE 19 submission at 12.

[13] While the Web has become synonymous with the Internet, it is one of a diverse range of applications that runs on and facilitates information exchange across the Internet. The Internet is the networking infrastructure that connects computers worldwide – in other words, the network of networks. Other Internet applications include e-mail, VoIP (Voice over Internet Protocol), mobile telephony, and peer-to-peer networks.

[14] See ARTICLE 19 submission at 12.

[15] See Free Software Foundation, "Keep DRM out of Web standards -- Reject the Encrypted Media Extensions (EME) proposal" (24 April 2013), *available at* https://static.fsf.org/dbd/Joint_Letter_on_W3C_HTML5_proposal.pdf. However, proponents claim that the specification will merely provide "a simple, easy to use way of putting encrypted content online." Tim Berners-Lee, "On EME in HTML 5" (28 February 2017), *available at* https://www.w3.org/blog/2017/02/on-eme-in-html5/.

[16] See World Wide Web Consortium, "Membership FAQ," *available at* https://www.w3.org/Consortium/membership-faq#who (stating "all types of organizations [including commercial, educational and governmental entities] and individuals").

[17] See W3C, Current Members," *available at* https://www.w3.org/Consortium/Member/List; see also DeNardis at 75.

[18] See W3C, "Membership Fees," *available at* https://www.w3.org/Consortium/fees (stating "W3C fees vary depending on the annual revenues, type, and location of headquarters of an organization").

[19] See W3C, "World Wide Web Consortium Process Document," § 3.3, *available at* https://www.w3.org/2017/Process-20170301/#Consensus.

[20] *Id*. at § 3.4.

Information and Communications Technologies.[21] ITU-T develops standards that "define how telecommunications networks operate and interwork", from landline networks to cable set top box architecture and broadband DSL.[22]

14. *Governance:* While these standards are non-binding and adopted on the basis of consensus, many of them have been widely adopted among States and the private sector. ITU membership comprises 193 States and more than 700 representatives from the private sector, non-governmental organizations, and academic institutions. Only States have voting rights.[23] However, non-State members may seek to influence the organization's proceedings and recommended standards through participation in each sector's Study Groups (which generates draft recommendations for adoption) and Sector Conferences (which define each sector's agenda and desired outcome every four or five years).[24] As the Internet supplants traditional telecommunications networks and systems, ITU's role in Internet standardization and governance is hotly contested. For example, ITU-T has established Study Groups focused on standardization for cloud computing and Internet of Things infrastructure.[25] Given that the ITU is an intergovernmental organization, however, some argue that its expanding role threatens the multi-stakeholder model of Internet governance that is critical to maintaining a free and open Internet.[26] Furthermore, ITU has drawn criticism for operating "a very exclusive, top-down decision making process", and lacking "transparency, openness, and inclusiveness".[27]

iv. European Telecommunications Standards Institute ("ETSI")

15. *What they do:* Unlike IETF, W3C, and ITU-T, which develop standards that apply globally, ETSI is a regional body focused on establishing European protocols for "fixed, mobile, radio, converged, broadcast and Internet technologies."[28] Nevertheless, these

[21] The other sectors are Radiocommunications (ITU-R), which allocates global radio spectrum and satellite orbits, and Telecommunication Development (ITU-D), which promotes the development of telecommunications infrastructure and services.

[22] International Telecommunication Union, "ITU-T Recommendations," *available at* https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx.

[23] ITU, "ITU World Telecommunication Standardization Assembly 2016: Background Paper" *available at* https://www.internetsociety.org/doc/itu-world-telecommunication-standardization-assembly-2016-background-paper.

[24] The ability to influence proceedings varies according to membership status. Becoming a non-state member of the ITU requires payment of membership fees, with different fees charged to private-sector, academic members, and non-governmental organizations. The membership fee for NGOs begins at 31,800 CHF. ITU, "Membership Fees," *available at* http://www.itu.int/en/ITU-T/membership/Pages/Categories-and-Fees.aspx. While there are other membership options available at slightly cheaper rates, these memberships do not afford the same rights as full sector members, and do not grant the right to influence final decision-making. ITU, "Can any company or organization become an ITU-T member?" *available at* http://www.itu.int/net/ITU T/info/answers.aspx?Fp=faqs.aspx&Qn=11&ewm=False; ITU, "Participation Rights," available at http://www.itu.int/en/ITU-T/membership/Pages/Rights.aspx.

[25] ITU, "ITU-T Recommendations," *available* at https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx*;* Telecommunication Standardization Sector of ITU, "Resolution 2-ITU Telecommunication Standardization Sector study group responsibility and mandates," *available at* https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.2-2016-PDF-E.pdf.

[26] See, e.g., Internet Democracy Project, "The ITU and global Internet governance," available at https://internetdemocracy.in/issues/global-internet-governance-architecture/the-itu-and-global-internet-governance/.

[27] ARTICLE 19 submission at 11.

[28] European Telecommunications Standards Institute, "About ETSI," *available at* http://www.etsi.org/about (last accessed February 28, 2017). ETSI also develops standards that "provide the technical detail necessary" to execute European Commission mandates and directives.

protocols often have global reach and impact. For example, before the advent of 3G and 4G networks, the GSM standard developed by ETSI was the de facto global standard for mobile communications.[29] ETSI also participates in the development of standards for next generation mobile networks as a member of the 3rd Generation Partnership Project.[30]

16. *Governance:* ETSI is registered as a non-profit organization composed of more than 800 members, including manufacturers, network operators, service and content providers, national administrators, universities and research bodies, user organizations, and consultancy companies and partnerships.[31] Membership is fee-based and open to "any company or organization, from any part of the world, with a legitimate interest in [ETSI's] work".[32] Proposals to create a new standard or to update an existing one may come from members, the European Commission, or the European Free Trade Association, and require the agreement of four members to proceed.[33] Depending on the type of standard involved, adoption may require the approval of a select committee of members, the entire membership, or the European National Standards Organizations.[34] Historically, ETSI has considered both international and national legal bases for human rights obligations when developing particular technical standards.[35]

v. Institute of Electrical and Electronics Engineers ("IEEE")

17. *What they do:* IEEE is the world's largest technical professional organization, composed of over 400,000 electrical engineers, computer scientists, and related professionals from more than 160 countries. The organization conducts standards development through its dedicated outfit, the IEEE Standards Association ("IEEE-SA"). IEEE standards span a wide range of fields, including aerospace, healthcare, transportation, nuclear power, and wired and wireless communications services.[36] IEEE has also been engaged in the development of standards for artificial intelligence and autonomous systems, and in April 2016, launched a global initiative to address the ethical dimensions of this work[37].

18. *Governance:* IEEE-SA members submit proposals for standards projects (known as "Project Authorization Requests"), which must gain the approval of a sponsor (usually the IEEE society responsible for the scope and content of a proposed standard) and the IEEE-

The European Telecommunications Standards Institute, "Different Types of ETSI Standards," *available at* http://www.etsi.org/standards/different-types-of-etsi-standards.

[29] ETSI, "Our standards," *available at* http://www.etsi.org/standards.

[30] See discussion *infra*.

[31] ETSI, "Who are our members," *available at* http://www.etsi.org/about/who-we-are.

[32] *Id.*; see also ETSI, "What Does Membership Cost?," *available at* http://www.etsi.org/membership/fees#Members.

[33] ETSI, "How does ETSI make standards?," *available at* http://www.etsi.org/standards/how-does-etsi-make-standards.

[34] *Id*.

[35] See, e.g., ETSI, "Security Techniques Advisory Group (STAG); A guide to the legislative and regulatory environment," §6.1, *available at* http://www.etsi.org/deliver/etsi_etr/300_399/330/01_60/etr_330e01p.pdf; see also ETSI, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)," §5.2, *available at* http://www.etsi.org/deliver/etsi_ts/187000_187099/187016/03.01.01_60/ts_187016v030101p.pdf.

[36] Institute of Electrical and Electronics Engineers – Standards Association, "Technology Standards & Resources," *available at* http://standards.ieee.org/findstds/index.html; see also DeNardis at 76. Note that some of the most widely known IEEE standards—including the Ethernet Local Area Network standards and the Wi-Fi family of standards— concern wired and wireless communications services.

[37] IEEE-SA, "IEEE Standards Association Introduces Global Initiative for Ethical Considerations in the Design of Autonomous Systems," *available at* http://standards.ieee.org/news/2016/ieee_autonomous_systems.html.

SA Standards Board to proceed.[38] Working groups are subsequently convened to develop and draft the relevant standard.[39] Once the sponsor has determined that "the draft of the full standard is stable," the standard is submitted for balloting.[40] The goal of balloting is to "gain the greatest consensus", and a standard will pass if at least 75 percent of all eligible ballots are returned and if 75 percent of these bear a yes" vote.[41]A 60-day public review process, which provides an opportunity for the general public to submit comments on the proposed standard, is initiated simultaneously with the balloting process.[42]After ballot approval, the standard is submitted to the IEEE-SA Standards Board for final approval.[43] While non-members are permitted to participate in certain standards projects, only members are eligible for leadership positions.[44] To participate in balloting, IEEE-SA membership or payment of a "per-ballot fee" is required.[45] Pricing for corporate membership is determined on the basis of annual revenues of the corporation, and each corporation is permitted only one vote on ballots.[46]

vi. The 3rd Generation Partnership Project ("3GPP")

19. *What they do:* 3GPP is a collaboration between seven telecommunications standards associations worldwide: The Association of Radio Industries and Businesses, Japan; the Alliance for Telecommunications Industry Solutions, USA; China Communications Standards Association; ETSI; Telecommunications Standards Development Society, India; Telecommunications Technology Association, Republic of Korea; and Telecommunication Technology Committee, Japan (known as "3GPP Organizational Partners").[47] 3GPP has developed standards for 3G and 4G networks, such as UMTS and LTE specifications respectively.[48] It is a key actor in the development of 5G standards – the next generation of mobile networks and wireless systems at the time of publication.[49]

20. *Governance:* The private sector has significant influence of the work of the 3GPP. Industry groups representing the interests of Telcos, ISPs, and related businesses may, at the invitation of an Organizational Partner, take part in 3GPP's activities as a Market Representation Partner. While the latter "does not have the capability and authority to define, publish and set [3GPP] standards", they may nevertheless "offer market advice to 3GPP and … bring into 3GPP a consensus view of market requirements" relating to

[38] IEEE-SA, "Develop Standards: Submitting A Project Request," *available at* https://standards.ieee.org/develop/par.html.

[39] IEEE-SA, "Develop Standards: What Is A Working Group?," *available at* https://standards.ieee.org/develop/wg.html.

[40] IEEE-SA, "Develop Standards: The Balloting Process," *available at* https://standards.ieee.org/develop/balloting.html.

[41] *Id*.

[42] IEEE-SA, "Develop Standards: The IEEE-SA Public Review Process," *available at* https://standards.ieee.org/develop/publicreview.html.

[43] IEEE-SA, "Develop Standards: How Is Final Approval Obtained?", *available at* https://standards.ieee.org/develop/finalapp.html.

[44] IEEE-SA, "IEEE-SA Membership," *available at* https://standards.ieee.org/membership/index.html. Non-members may participate in the individual standards development process, but not the entity standards development process. See IEEE-SA, "FAQs: The Entity Standards Development Process," *available at* https://standards.ieee.org/faqs/cmm.html.

[45] IEEE-SA, "Develop Standards: The Balloting Process," *available at* https://standards.ieee.org/develop/balloting.html.

[46] IEEE-SA, "IEEE-SA Membership," *available at* https://standards.ieee.org/membership/index.html; *Id*.

[47] 3rd Generation Partnership Project, "Partners," *available at* http://www.3gpp.org/about-3gpp/partners.

[48] 3GPP, "Specifications Home," *available at* http://www.3gpp.org/specifications/specifications.

[49] 3GPP, "About 3GPP," *available* at http://www.3gpp.org/about-3gpp.

relevant telecommunications services, features, and functionalities. Notably, it does not appear that 3GPP provides similar opportunities for civil society, human rights groups, academics and others to provide input on the human rights impact of their work.

B. Incorporating Human Rights Considerations into Standards Development

21. The Special Rapporteur has joined a growing body of technical, academic and civil society experts calling for in-depth study of the human rights impact of technical standards and how standards development should seek to enable the exercise of human rights. While the current discourse largely focuses on the IETF's protocol design process, the key questions and issues discussed cut across all forms of standards development.

22. A survey of the relevant literature reveals a variety of approaches concerning the role of human rights in standards development, but two are particularly salient.[50] Some argue that the protocol design process should "bak[e]" into the architecture those "key, universal values" reflected in the Universal Declaration of Human Rights.[51] These human rights standards are widely accepted among the international community, even if their interpretation and implementation vary across social, political, and cultural contexts. In particular, values that are most relevant to protocol design and have a "fundamental impact on individual autonomy", such as freedom of expression and privacy, are "protected in the constitutions of many countries" and have "widespread democratic assent".[52]

23. Others, however, insist that protocol design should ensure that architecture design is flexible enough to accommodate a range of outcomes, including those that may be inconsistent with human rights, so that "the tussle takes place within the design".[53] In this view, limited understanding of the precise content of human rights and their accompanying parameters is a critical barrier to instantiating human rights through standards development.[54] Furthermore, since SDOs have neither the expertise nor legitimacy to make

[50] There are at least three other proposed approaches in the field: 1) design that, while not explicitly referencing human rights, nevertheless treats the Internet backbone as a public good and seeks to guarantee its "overall integrity and functionality"; 2) design that proceeds on the basis that Internet access (and potentially other Internet-related capacities) is in and of itself a human right; and 3) a 'wait-and-see' approach that supports more human rights education in the technical community but cautions against any definitive claims concerning the design process pending further research. For a fuller summary of these approaches see Niels ten Oever & Corinne Cath, Human Rights Protocol Considerations Research Group, IRTF, "Research into Human Rights Protocol Considerations," draft-irtf-hrpc-research-13 (May 18, 2017) *available at* https://tools.ietf.org/html/draft-irtf-hrpc-research-13. Additionally, the Human Rights Protocol Considerations Research Group, led by ten Oever and Cath, also proposes its own approach to incorporating human rights into protocol design, which is discussed *infra*.

[51] Ian Brown, David D. Clark, & Dirk Trossen, "Should Specific Values Be Embedded in the Internet Architecture," (2010) *available at* http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf.

[52] *Id*.

[53] David. D. Clark, John Wroclawski, Karen R. Sollins, and Robert Braden, "Tussle in cyberspace - defining tomorrow's Internet", IEEE/ACM Transactions On Networking, Vol. 13, No. 3 (June 2005) at 466, *available at http://dl.acm.org/citation.cfm?id=1074049*.

[54] Corinne Cath & Luciano Floridi "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights" L. Sci Eng Ethics (2017) 23: 449, *available at https://link.springer.com/article/10.1007/s11948-016-9793-y*.

or interpret human rights standards, such activity may trigger governments to abandon the current standards process, "effectively cleaving the Internet at the logical layer".[55]

i. The human rights impact of technical standards

24. These concerns require SDOs to tread cautiously, and may counsel against "hard-coding human rights into protocols".[56] However, they do not diminish the close connection between standards development and the exercise of human rights online. Like any technological development, standards do not simply serve technical functions. Instead, they are shaped by their historical and cultural contexts, reflect the assumptions and values of their respective developers, and influence public policy.[57]

25. Wittingly or not, the protocol design process already incorporates human rights values to varying degrees. For example, standards development focused on Internet accessibility for minorities and other vulnerable groups – such as the W3C's Web Accessibility Initiative to enhance web access for those with cognitive and physical disabilities – enhances their capacity to exercise freedom of expression online.[58] Edward Snowden's revelations about mass government surveillance have also prompted deeper scrutiny of the privacy implications of protocol design choices. In 2013, the Internet Architecture Board adopted guidance to "make designers, implementers, and users of Internet protocols aware of privacy-related design choices.[59] While the guidance approaches privacy breaches as "technical attack[s] that undermin[e] trust in the network", it nevertheless facilitates the exercise of the right to privacy and related human rights.[60]

26. Conversely, inadequate consideration of human rights has contributed to technical loopholes that render users vulnerable to access restrictions, privacy violations, and other human rights abuses. For example, the visibility of source and destination IP addresses in the IPvV4 protocol – a widely used protocol for data communication across different networks – has enabled censors to identify websites and network traffic for blocking or discrimination[61] The lack of mandated Transport Layer Security (TLS) under HTTP connections has not only exposed users to third party interception of their communications, but also deliberate attempts to compromise the security of their devices.[62]

ii. Standards development and human rights considerations

27. While it is not always possible to encode human rights values during the protocol design process, developers and other stakeholders should nevertheless be sensitive to the human rights implications of their work. The perceived lack of expertise and legitimacy is not insurmountable. The business and human rights movement, which has navigated similar challenges, demonstrates that non-State are capable of adopting an incremental and credible approach to human rights accountability. In particular, SDOs may seek guidance from ICT companies that have adopted due diligence and responsibility-by-design measures as part of

[55] Jonah Force Hill, "A balkanized Internet? The uncertain future of global Internet standards," Georgetown Journal of Int'l Affairs, November 2, 2014, *available at* *http://journal.georgetown.edu/wp-content/uploads/2015/07/gj12707_Hill-CYBER-2012.pdf*.

[56] draft-irtf-hrpc-research-13 at 11.

[57] See, e.g., Sandra Braman, "Internet Designers as Policy-Makers," (February 21, 2017) *available at* https://cyber.harvard.edu/events/luncheons/2017/02/Braman.

[58] DeNardis at 77-82.

[59] A. Cooper, H. Tschofenig, B. Abob, J. Peterson, J. Morris, M. Hansen, R. Smith Janet, Internet Architecture Board (IAB), RFC 6973 (July 2013), *available at* https://tools.ietf.org/html/rfc6973*;* Internet Society submission at 4.

[60] Cath & Floridi at 458; Internet Society submission at 6.

[61] draft-irtf-hrpc-research-13 at 21-22.

[62] draft-irtf-hrpc-research-13 at 26-27.

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),

Patrik Hiselius (Telia Company), Rikke Frank Jørgensen (Danish Institute for Human Rights), Nicole Karlebach (Yahoo), Molly Land (University of Connecticut), Rebecca MacKinnon (Ranking Digital Rights), Peter Micek (Access Now), Charles Mok (Hong Kong Legislative Council), Laura Okkonen (Nokia), Moira Oliver (British Telecom); Milka Pietikainen (Millicom), Lucy Purdon (Privacy International), Michael Samway (Georgetown University), David Sullivan (Global Network Initiative), Niels ten Oever (ARTICLE 19), Alexandria Walden (Google), Richard Wilson (University of Connecticut), and Cynthia Wong (Human Rights Watch).

93. The consultation was made possible by the financial support of the University of Connecticut's Humanities Institute, School of Law, and Human Rights Institute.

94. The report reflects points raised during the consultation but does not necessarily reflect the views of the Special Rapporteur or all participants.

A. Session 1: Identifying Human Rights Risks

95. In this session, participants discussed the variety of risks to human rights that Telcos, ISPs, vendors, and others may encounter in their daily operations, both in terms of compliance with local law as well as risks associated with the development of products, services and business strategies.

i. Engaging more actors

96. There was a general consensus among participants that the discussion about human rights risks should include actors beyond Telcos and ISPs, such as vendors, IXPs, and submarine cable providers.

97. Participants noted, hwoever, that it was less clear how to evaluate the human rights responsibilities of vendors, and that an understanding of how they operate and network equipment technology would be essential. It was agreed that these companies present unique challenges and there was a need for a more concrete understanding of the human rights risks their businesses face or create, ongoing efforts to address them, and accountability gaps.

98. Participants suggested that submarine cable providers should be more transparent regarding their contracts and their arrangements with governments. They noted several issues of specific concern, including: (i) Do Telcos / ISPs require minimal standards on the integrity/authenticity of the interface with submarine cable providers? (ii) What is the nature of the submarine cable provider's responsibility to secure the cables? (iii) Are there human rights issues associated with the cutting of cables? (iv) What are the terms of the contractual relationships and which actors are involved?

ii. Imprecise or vague legal standards

99. Participants emphasized the risks associated with imprecise or vague legal standards governing censorship and surveillance.

100. Concern was raised, for example, about the vague and open-ended nature of cybercrime laws that ban "disturbing", "annoying", or "inciting" online content, which are employed to censor and chill expression online. Reform of these laws should take into account how they are being enforced. How companies interpret and implement these laws is also critical.

101. One participant recommended that companies should work with the Global Network Initative ("GNI") to lobby for meaningful limits on content regulation and surveillance laws.

iii. Requests for website blocking and access to users' data

102. Participants noted that governments frequently demand that Telcos and ISPs block websites and hand over communications content and metadata, often without a valid judicial order.

103. Participants suggested that governments should be more transparent about their content takedown and surveillance requests, and should provide transparency reports on the volume and scope of such requests, and the number of such requests made with a warrant.

104. Participants mentioned that some ISPs integrate procedural safeguards into their licensing contracts, specifying, for example, the procedural steps to be followed when a government requests website blocking or access to user data. It was suggested that more companies should do this and perhaps go even further in specifying that requests must be in writing, signed by a responsible individual, identify the legal basis for the request and the time period for implementations, and set out the process for challenging the request.

105. Participants suggested that companies track the number of requests received for website blocking or access to user data, the identity of the requesting entity, the nature of the request, and the form of the request. They mentioned that such practice will make it easier to identify relevant, observable trends over time and will also allow the company to communicate to stakeholders transparently about its efforts to addres its human rights impacts.

106. Participants also expressed concern that customers and users are not aware of their rights. When local Telcos and ISPs do not themselves value transparency, participants noted that consumers are likely unaware of their rights and of the company's record. They suggested that advocacy groups should do more in term of public education efforts.

B. Session 2: Due Diligence Practices and Procedures

107. In this session, participants discussed the practices and procedures that Telcos, ISPs, and vendors might employ to assess and address their human rights risks and impacts.

i. Standardization

108. Some participants expressed the need to have a clear set of standards with regard to due diligence. The lack of agreed upon standards makes it harder for companies to report data that can be compared across the industry.

109. Some argued in favor of concrete guidance for how companies engaged in Internet and telecommunications access should implement the United Nations Guiding Principles on Business and Human Rights ("UN Guiding Principles").

110. Others argued that it would not be possible to have a standardized due diligence process across the industry or even a particular category of actors (e.g. among Telcos), since each company may have different needs, responsibilities, organizational structures, and internal processes.

111. Participants noted that, at a minimum, companies should disclose their policies and practices to ensure respect for human rights.

ii. What is Due Diligence?

112. Participants first considered the definition of due diligence, the scope of activities covered, and the relationship between due diligence and Human Rights Impact Assessments ("HRIA").

113. Many participants agreed that a company should publicy announce its commitments to the UN Guiding Principles. However, this alone is not sufficient. Companies must also

follow up on their commitments by translating these principles into due diligence policies and practices that are triggered during relevant business activities, such as the design and engineering phase of a new product, product modification, or market entry. Companies should ensure that due diligence is conducted not only by employees but also relevant corporate partners and agents.

114. Several participants agreed that robust due diligence include at least the following steps: (i) analysis of governing human rights laws and standards, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the UN Guiding Principles, and the GNI Principles; (ii) understanding the human rights landscape of the relevant market with particular focus on rule of law, freedom of expression and privacy; (iii) considering the impact of relevant local laws on freedom of expression and privacy; (iv) connecting business plans to potential human rights risks and opportunities; (v) considering how the product could promote human rights, for example by enhancing access, education, communication, or privacy; (vi) evaluating the risks based on the company's products and operations, including the severity and likelihood of the risks, in consultation with stakeholders; and (vii) developing a strategy for mitigating risks and protecting human rights.

iii. Human Rights Impact Assessments

115. Participants discussed HRIAs as a means of due diligence. HRIAs inform and guide evolving corporate strategies to ensure respect for their customers' right to freedom of expression and privacy.

116. Some noted that while HRIAs have been promoted as a due diligence tool, there should be a better shared understanding of what precisely these assessments require or entail.

117. Participants suggested companies may appear to be more credible if HRIAs are outsourced to an independent expert or body of experts.

iv. Why Due Diligence?

118. Participants discussed how due diligence can contribute to effective risk management.

119. Due diligence may integrate a more rights sensitive culture within the company, mainstreaming human rights considerations within corporate thinking and decision-making.

120. Companies might develop greater ownership of their human rights performance as they consider the human rights issues they face during the process of policy development and reflection on existing practice, rather than primarily engaging with human rights only when they are subject to external challenge.

v. When to Conduct Due Diligence?

121. Participants also discussed how often a company must engage in due diligence.

122. Participants emphasized that due diligence should be conducted regularly and on an ongoing basis, and not simply to address one-off events. Ongoing due diligence enables a company to understand how its risks can change over time and how to manage them effectively.

123. Participants identified the need for more clarity on the types of business activities that trigger due diligence, and greater corporate transparency concerning these triggers. Triggers could include changes in the political environment, new laws, contract renewals, change of service, or market entry.

124. Mergers and acquisitions are also a trigger point, although one participant pointed out that it might be difficult to conduct due diligence in the context of a contractual negotiation, since the only information provided is public information. Therefore, it might be more appropriate to conduct post-acquisition due diligence.

125. It is essential to address human rights issues at the earliest stages of business relationships to minimize situations where the company has little leverage to mitigate or avoid adverse human rights impacts.

126. Participants also noted the importance of due diligence in terms of the design of products and services.

vi. Who is Part of Due Diligence?

127. Participants discussed the types of employees and internal teams that should be engaged in due diligence processes – these include senior management, cross-functional human rights teams with senior oversight, investors, and external stakeholders.

128. A number of participants supported the involvement of senior management, which sets the tone throughout the company. At a minimum, the board of directors, corporate executive officers, and other senior executives should actively support the company's commitments to human rights and understand their own roles and responsibilities in ensuring the company fulfils its commitments in this area.

129. Participants also agreed that due diligence should be conducted by cross-functional human rights teams with senior oversight, and include employees from the legal, policy, business functions, and engineering teams. Such teams send a signal that human rights concerns are the responsibility of the entire business enterprise. One participant noted that such teams should be led by employees with human rights expertise.

130. Engineers are particularly important because they have technical expertise concerning the company's products and services, and can significantly inform the design of technology-oriented approaches to mitigating or preventing adverse human rights impacts (such as design modification).

131. A specialized human rights team not only facilitates rapid responses to human rights crises, but also enhances the company's ability to pre-empt and avoid such crises.

132. A few participants noted that investors can play a very important role in incentivizing companies to recognize their human rights risks.

133. Participants also suggestd that external stakeholdesr should be involved in the due diligence process. Ongoing interaction and dialogue between a company and affected stakeholdesr, such as civil society representatives and other rights holders, enable the company to respond to their interests and concerns.

vii. Transparency

134. Several participants emphasized the need for greater corporate transparency concerning internal due diligence processes and practices – at a minimum, companies should disclose when they conduct due diligence, and high level summaries of the HRIA results.

viii. Outstanding Issues

135. Participants identified the following questions and issues that require further discussion: (i) How should a company with diversified services and multiple business models identify due diligence triggers and standardize due diligence processes across its operation? (ii) What are the costs (financial, time and otherwise) associated with due diligence? (iii) How much weight does / should a company assign to due diligence findings

and recommendations in their overall decision making process? (iv) What other trigger points exist beyond compliance with government requests? (v) When companies are already established in a market that poses human rights concerns, what can they do to mitigate or prevent adverse human rights impacts? How can they support rights-oriented legal and policy reforms?

C. Session 3: Remedies

136. In this session, participants discussed the types of remedies that should be available to Internet users when their human rights are violated.

i. The Government's Role

137. The role of the government in providing or facilitating access to an effective remedy was discussed.

138. In addition to the UN Guiding Principles, participants noted that European Court of Human Rights jurisprudence provides guidance on the content of the right to an effective remedy. According to the Court, an effective remedy requires recognition of the violation, the provision of satisfaction or compensation, and the establishment of sufficient grounds to avoid its recurrence.

139. Several participants noted that, under the UN Guiding Principles, the State bears the primary duty to ensure remedies; however, most States have not paid sufficient attention to this pillar of the UN Guiding Principles.

140. Others emphasized that the UN Guiding Principles also recognize a role for non-State remedies: Without a remedy provided by the State, rights holders often have to rely on the company.

141. Participants noted that Telcos and ISPs operate in a complex domestic and international legal system with various avenues for remedy. These include State-based judicial mechanisms, international organizations such as the OECD (Organization for Economic Co-operation and Development), national human rights institutions, and multi-stakeholder initiatives. One participant suggested that OECD's national contact points also provide a mechanism to bring human rights complaints against companies.

ii. Jurisdiction

142. Participants noted that the frequently cross-jurisdictional nature of human rights violations on the Internet complicates the ability of both State and non-State actors to provide an effective remedy.

143. Most countries' domestic legal frameworks give greater protection to the privacy rights of citizens than non-citizens, but the obligation of states to respect rights is not limited to the rights of persons physically in their territory.

144. Participants noted, however, that this view is contested and some governments have denied that their obligations extend to actions undertaken outside their territory. At the very least, however, territorial jurisdiction may arise on the basis of physical location or where the data is processed.

iii. Types of Remedies

145. The types of remedies that might be appropriate for human rights violations by Telcos, ISPs and associated companies was the subject of considerable discussion.

146. Participants noted that there are many different types of remedies including but not limited to recognition, satisfaction, non-repetition of violations, compensation, and

restitution. The remedy must be proportional to the harm. Participants also discussed the use of individual versus collective remedies.

147. Other participants noted that other kinds of remedies may be appropriate, such as disclosing information about the violations (such as HTTP 451, a landing page that explains why a webpage is unavailable), or commitments to non-repetition. In the ICT context, many victims are not seeking compensation; instead, they would rather be restored to the place they were before the violation.

148. Participants observed the importance of transparency concerning the violation in order to enable access to an effective remedy. Privacy concerns, however, may limit transparency. Furthermore, since many violations are triggered by local laws and other forms of State action, an appropriate remedy might require revealing the State's role – disclosures that many companies are unable or unwilling to make.

149. Remedies may be judicial or non-judicial, and non-judicial remedies may be integrated into a self-regultaory process. The GNI, for example, may provide a venue for the design and implementation of appropriate remedies.

iv. Grievance Mechanisms

150. Participants discussed the procedural elements of a grievance mechanism.

151. Participants suggested that companies should create grievance mechanisms to address users' complaints about potential human rights violations. Several GNI member companies have made commitments to establish grievance mechanisms.

152. One participant suggested that pre-existing complaints or whistleblowing hotlines provide a model for human rights grievance mechanisms. However, any channel of communication between the company and its users should be adequately secure and accessible.

153. Some ISPs have created a whistleblowing system to deal with corruption, and this could also be used to address human rights violations.

v. Other Issues and Challenges

154. Some participants noted that it could be difficult in some situations to identify the harms for which a company should be responsible. Under what circumstances is a company responsible? Under what circumstances should they provide a remedy? How closely related must the harm be to their activities?

155. Several discussed the distinction between human rights harms and non-human rights harms. Does the obligation to provide a remedy extend to both? How should these be distinguished? Participants noted, for example, that it is unclear whether a company should be responsible for economic harms arising from a government-ordered shutdown.

156. The large number of complaints that companies receive also poses logistical challenges. Additionally, a large number of complaints require translation, and raises issues of political, cultural and social context.

157. A few participants were also concerned that a narrow conception of remedies my disincentivize companies from making the structural changes needed to prevent or mitigate future violations.

158. Participants also asked about the role of the investor. A participant suggested that investors should be urged to create a socially responsible investment fund.

D. Session 4: Transparency

159. Participants discussed the need for companies to disclose information that meaningfully informs users about the human rights risks and harms associated with their products and services.

i. The Value of Corporate Transparency

160. Several participants discussed the importance of making a case to companies that transparency can be good for business. Transparency can be a boon to a company's brand. Healthy competition between companies about what they disclose and how effectively they disclose such information may meaningfully enhance transparency. Companies that face significant risks to their reputation in the event of non-disclosure are naturally inclined to innovate in this area.

161. Those pushing for heightened corporate transparency, however, must be sensitive to the need to protect trade secrets and the legal and regulatory environment in which these companies operate.

162. New companies require guidance on the need to create transparent due diligence processes and other transparency measures from the outset.

163. Current transparency practices concerning due diligence processes were also discussed. Some companies disclose information about HRIAs but others do not even disclose the fact that they conduct assessments. Companies should at least disclose when they perform HRIAs, and a summary of high-level findings.

164. Companies also play a critical role in pushing governments for more transparency.

ii. Challenges to Corporate Transparency

165. Participants discussed challenges concerning transparency reporting and standards.

166. Many participants agreed that minimum standards of disclosure should be established. However, these should not be so rigidly defined that they become a check-the-box process and deter transparency innovation.

167. Transparency reporting is insufficient. In addition to regular reporting, companies should also address the need to make disclosures in real time that respond to rapidly evolving situations (such as complicated product rollout or an evolving crisis).

168. Areas where corporate transparency can be improved include: information concerning the number of and reasons for website blocking and network shutdown incidents (including copyright takedowns and private defamation claims); the human rights implications of mergers and acquisitions; human rights risks associated with the use or misuse of products or services; and the nature and frequency of security updates, among others.

iii. Transparency Standards for Vendors and Submarine Cable Providers

169. The comparative lack of transparency measures for companies other than Telcos and ISPs was discussed.

170. Participants were concerned that non-consumer facing companies, such as vendors and submarine cable providers, have less incentive to adopt transparency measures. Submarine cable providers in particular have reportedly expressed skepticism concerning the relevance of human rights to their business. Companies that specialize in the design and sale of surveillance and monitoring equipment may have even less incentive to be transparent about their customers and practices.

171. Vendors are no longer simply selling routers and switches, but also network monitoring systems (e.g. Deep Packet Inspection) and associated training and consultation services. The human rights risks associated with these products and services require further study and analysis, and it is unclear whether and how vendors conduct human rights due diligence during their design and sale.

172. Forensic analysis of products currently on the market may reveal design flaws and security risks. Open-source design efforts may also mitigate human rights risks associated with “closed” systems.

173. For submarine cable providers, it might be helpful for civil society and the public to access cable leasing contracts, the parties that have access to a cable, and the circumstances under which cables may be cut or otherwise interfered with.