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 excutives 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.