



November 1, 2016

David Kaye

Special Rapporteur on the right to freedom of opinion and expression

Office of the United Nations High Commissioner for Human Rights

Geneva, Switzerland

freedex@ohchr.org

RE: Submission on Freedom of Expression and the Telecommunications and Internet Access Sector

The Telecommunications Industry Dialogue (Industry Dialogue) is pleased to provide input to the Special Rapporteur's study on freedom of expression in the telecommunications and Internet access sector.

The Industry Dialogue is a group of telecommunications operators and vendors who jointly address freedom of expression and privacy in the telecommunications sector in the context of the UN Guiding Principles on Business and Human Rights. These companies have a global footprint, providing telecommunications services and equipment to consumers, businesses, and governments in nearly 100 countries worldwide. In March of 2013, the Industry Dialogue adopted a set of Guiding Principles, which explore the interaction and boundaries between a government's duty to protect human rights and the corporate responsibility of telecommunications companies to respect human rights.¹

I) Trends in Laws, Regulations, and Other Extralegal Measures Affecting Business's Ability to Respect Freedom of Opinion and Expression

Country Legal Frameworks Pertaining To Freedom of Expression and Privacy in Telecommunications

Companies participating in the Industry Dialogue work to respect the freedom of expression and privacy rights of their users and customers while complying with local law and protecting the safety of company personnel. In each of the markets in which they are present, licensed telecommunications operators are bound by laws and regulations that govern how the

¹ See <http://www.telecomindustrydialogue.org/about/guiding-principles>.

² Information on Country Legal Frameworks Pertaining to Freedom of Expression and Privacy in Telecommunications available at <http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/>.

³ See <http://www.teliacompany.com/globalassets/telia-company/documents/about-telia->



authorities may intercept communications, obtain access to communications data, restrict the content of communications, take control of networks during emergencies, or suspend services. The pertinent legal framework(s) may be contained in a variety of different norms and may not be subject to uniform interpretation.

In light of this complexity, and in the interest of contributing to constructive dialogue with stakeholders, the Industry Dialogue's Guiding Principles state the aim of participating companies to compile and make available guidance and information on the main laws, regulations and standards that are applicable to licensed operators, for informational purposes.

The Industry Dialogue website brings together information published by Vodafone Group in June of 2014 and February of 2015 and by Telenor Group in May of 2015 with additional material that the Telecommunications Industry Dialogue published in June of 2015.² In addition to the aforementioned company reports covering the pertinent legal frameworks in 39 countries, the Industry Dialogue published reports on five countries – Colombia, Jordan, Kazakhstan, Pakistan, and Russia – that represent the diversity of its member companies' global footprint. Over time, the Industry Dialogue and its participating companies aim to expand on this resource. Recently, Telia Company has done so by publishing a list of the most relevant laws on signals intelligence and real-time access to communications in 15 markets in which the company has majority-owned operations.³

The information contained in this resource seeks to highlight some of the most important legal powers available to government authorities seeking to access communications data or to restrict the content of communications in 44 different countries. These powers are divided into the following six categories: 1) provision of real-time, lawful interception assistance, 2) disclosure of communications data, 3) national security and emergency powers, 4) censorship-related powers, 5) oversight of the use of these powers, and for certain countries, 6) publication of laws and aggregate data relating to lawful intercept and communications data requests.

The Industry Dialogue selected the law firm Hogan Lovells International LLP to perform its reports, using the same methodology that the firm employed in preparing reports for Vodafone Group and Telenor Group. Hogan Lovells attorneys worked with local counsel in the five countries covered to compile and interpret the relevant laws and to present them in a manner that is accessible to all interested parties.

² Information on Country Legal Frameworks Pertaining to Freedom of Expression and Privacy in Telecommunications available at <http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/>.

³ See http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/ledr_oct2016_final.pdf.



Clear laws that respect international conventions and narrowly define by whom, how and in what circumstances law enforcement requests can be made are crucial to protect privacy and free expression. Clear laws and processes are also crucial tools for telecommunications companies to respect privacy and freedom of expression of our customers. This is not because a company's responsibility for these rights starts and ends with the law, but because clear laws promote accountability for all parties.

What the legal frameworks resource published by the Industry Dialogue shows is that in many cases, countries are falling short of such clear and rights-respecting frameworks.

Network Shutdowns

The Industry Dialogue and GNI are deeply concerned by the increasing number of government orders to shut down or restrict access to communication networks and related services around the world. Both organizations issued a joint statement on this issue in July 2016.⁴

Government-mandated disruptions of communications networks, network services (such as SMS), or internet services (such as social media, search engines, or news sites) can undermine security and public safety, threaten free expression, restrict access to vital emergency, payment and health services, and disrupt contact with family members and friends. In some countries, the orders frequently occur at politically sensitive moments, during unrest or in the lead-up to elections, restricting the free flow of information.

The protection of national security and public safety are important government concerns. Network shutdowns, and the wholesale blocking of Internet services, however, are drastic measures that often risk being disproportionate in their impact. Governments who employ these measures often do so without justifying them as necessary and proportionate under international human rights standards.

Clear, precise and transparent legal frameworks regarding government authority to restrict communications do not exist in all states, and provisions for adequate, independent oversight are often absent. Such safeguards are critical to ensure restrictions are strictly necessary and proportionate. Where the rule of law is weak, these orders can present even greater human rights risks.

⁴ Global Network Initiative and Telecommunications Industry Dialogue Joint Statement on Network and Service Shutdowns, available at <http://www.telecomindustrydialogue.org/global-network-initiative-telecommunications-industry-dialogue-joint-statement-network-service-shutdowns/>.



Direct Access

As highlighted in the Industry Dialogue's submission to your previous report, as a condition of operating in numerous countries, some governments may require direct access into companies' infrastructure for the purpose of intercepting communications and/or accessing communications-related data. This can leave the company without any operational or technical control of its technology. While in countries with independent judicial systems actual interception using such direct access may require a court order, in most cases independent oversight of proportionate and necessary use of such access is missing.

Your predecessor, Frank La Rue, and the European Court of Human Rights have both recommended that states refrain from imposing such a requirement on business enterprises. Governments may also use surveillance technology other than internationally standardized lawful interception technology, independently, in order to gain access to user data without the knowledge of telecommunications operators. It is the position of the Industry Dialogue that government agencies should be required to obtain assistance from companies when they exercise their lawful powers to access communications data in accordance with international standards; e.g., companies should retain the operational and technical means of giving it.

Good Practice on the Lawful Disruption of Access to Online Services

The restriction of online content interferes with the right to freedom of expression and should satisfy the tests of legality, necessity, and proportionality established in Article 19 of the International Covenant on Civil and Political Rights. The Industry Dialogue welcomed the Australian government's draft guidelines for the use of section 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services, e.g. the blocking of websites, which if adopted, would constitute important and substantial progress toward protecting the right to freedom of expression online.⁵

In a submission to the Australian government consultation on these guidelines, the Industry Dialogue made the following comments reflecting elements of good practice in the government's draft guidelines:

- **Commending the requirement that a government agency head must authorize the blocking of websites and that senior government officials should approve individual blocking requests.**

⁵ Submission to the Australian Government draft guidelines for the use of section 313(3) of the Telecommunications Act 1997, available at <http://www.telecomindustrydialogue.org/wp-content/uploads/ID-Input-to-Australian-Guidelines-3.pdf>.



- **For each agency to publish its policies and procedures governing requests to disrupt access to online services.** The Industry Dialogue encourages agency authorities to ensure that these documents are carefully crafted to be consistent with the guidelines and other applicable law. It may also be useful to consult in advance with ISPs about such policies and procedures. This will help to ensure that companies can respond quickly and within the bounds of applicable laws when an agency actually issues a blocking request. The automatic expiration of blocking requests after a certain time period is also a welcome guideline.
- **Limiting blocking to cases involving serious criminal or civil offenses or threats to national security and would provide agencies with a list of factors to consider prior to making requests.** This helps to ensure that restrictions of online content are a necessary and proportionate means of achieving a legitimate aim.
- **The use of landing pages to inform Internet users when content has been restricted pursuant to a government request.** And the guidelines' list of specific information to be included in such landing pages will provide meaningful transparency for those encountering blocked websites and those seeking review of blocking decisions. Privacy needs to be protected in the setup of landing pages. The Industry Dialogue also welcomes greater disclosure regarding requests to disrupt access to online services, both at the time when individual requests occur and through the annual reporting of statistical information on the aggregate number of requests.
- **Commending the requirement that agencies establish complaint and review processes that allow affected parties to contest a decision to disrupt access.** The Industry Dialogue applauds this as consistent with the recommendations of the UN Human Rights Committee and other human rights experts.
- **Consultation with technical experts and Internet service providers prior to requesting the disruption of access to online services.** The Industry Dialogue notes that this will facilitate the restriction of content in a targeted manner that is more likely to be consistent with the applicable principles of necessity and proportionality.

II) Business Policies, Processes and Practices to Prevent, Mitigate or Challenge the Human Rights Impact of State Laws or Actions that Suspend or Restrict Access to Communications or Provide Access to Customer Data

The Industry Dialogue is based on a set of Guiding Principles addressing freedom of expression and privacy as they relate to the telecommunications sector. We have included here examples of how companies are implementing the Guiding Principles in their operations in response to freedom of expression challenges. These principles also address company policies



and practices to promote transparency and provide remedy. The below table provides examples of implementation by Industry Dialogue companies.⁶

Telecommunications companies should, to the fullest extent that does not place them in violation of domestic laws and regulations, including license requirements and legal restrictions on disclosure:

Guiding Principle	Examples of Industry Dialogue Implementation
<p>1. Create relevant policies, with Board oversight or equivalent, outlining commitment to prevent, assess and mitigate to the best of their ability the risks to freedom of expression and privacy associated with designing, selling and operating telecommunications technology and telecommunications services.</p>	<p>AT&T issued its Human Rights in Communications Policy in the fall of 2010, after it was approved by senior executives and presented to the Public Policy and Corporate Reputation Committee of the AT&T Board.⁷ The Policy sets out AT&T’s commitment to respect human rights, affirming that the freedom to access information, the freedom to communicate and the respect for personal privacy are essential to the advancement of human potential.</p> <p>Following the merger and acquisition of Alcatel-Lucent, Nokia reviewed and updated its’ Human Rights Policy, which was published in October 2016 and reinforces the company’s commitment to human rights, including the right to privacy and freedom of expression and assembly.⁸</p> <p>Telia Company adopted a Group Policy on freedom of expression in telecommunications, based on an external human rights impact assessment and on the ID Guiding Principles, in December 2013, updated in September 2015.⁹ The Policy addresses Telia Company’s commitments in relation to requests or demands with potentially serious impacts on freedom of expression in telecommunications, i.e. targeted surveillance in exceptional cases; mass surveillance where authorities demand unrestricted real-time network access; shutdown of all or parts of a network; blocking or restricting access to specific services, websites or content; blocking or restricting individual customers’ access to services or networks;</p>

⁶ Reporting by each company of their implementation of the Guiding Principles is available on the Industry Dialogue website at <http://www.telecomindustrydialogue.org/about/implementing-the-guiding-principles/>.

⁷ http://about.att.com/content/dam/csr/FAQpdfs/Human_Rights_Communications_Policy.pdf.

⁸ http://company.nokia.com/sites/default/files/download/nokia_group_human_rights_policy.pdf.

⁹ http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/public-policy/telia-company_group-policy_freedom-of-expression-in-telecommunications.pdf.



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>obligations to transmit mandatory communications issued by the government authorities; and proposals for new laws or significant imposed operational changes. The Policy was introduced on board level in all majority-owned companies, followed by local board decisions to adopt the policy and its adhering instruction and publishing of the policy on their respective local website.</p> <p>Vodafone closely manages and monitors compliance with legal obligations and its relationship with law enforcement authorities to address respect for human rights. Vodafone’s Privacy Commitments and Global Policy Standard on Law Enforcement Assistance, with Executive Committee sponsorship, set out the requirements for balancing the potentially conflicting requirements of respecting privacy and assisting law enforcement.¹⁰ These outline that accountability is held at the most senior level. In 2015/16, Vodafone updated its Code of Conduct to expand its references to human rights.¹¹ The relevant section states: “We respect all internationally proclaimed human rights, including the International Bill of Human Rights and the principles concerning fundamental rights set out in the International Labour Organization’s Declaration on Fundamental Principles and Rights at Work. We strive to ensure that we are not complicit in human rights abuses. We shall, in all contexts, seek ways to honour the principles of internationally recognised human rights, even when faced with conflicting requirements. We are also committed to implementing the United Nations Guiding Principles on Business and Human Rights throughout our business operations.”</p> <p>Telefónica includes in its Business Principles the right to privacy as the foundation for a trust-based relationship with our stakeholders since 2010. Likewise, the Telefónica Group approved a Privacy Policy and has a strong commitment to human rights since 2013.¹²</p>

¹⁰ Vodafone privacy commitments available at <http://www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/privacy-and-security.html#cs2>; Vodafone Global Policy Standard on Law Enforcement Assistance available at <http://www.vodafone.com/content/dam/vodafone/about/sustainability/lawenforcementassistance.pdf>.

¹¹ <http://www.vodafone.com/content/index/about/conduct.html>.

¹² <http://annualreport2014.telefonica.com/sites/default/files/documentos/sustainability-report.pdf>.



Guiding Principle	Examples of Industry Dialogue Implementation
<p>2. Conduct regular human rights impact assessments and use due diligence processes, as appropriate to the company, to identify, mitigate and manage risks to freedom of expression and privacy – whether in relation to particular technologies, products, services, or countries – in accordance with the Guiding Principles for the implementation of the UN Protect, Respect and Remedy framework.</p>	<p>In October 2016, Telia Company released a summary report, Human Rights Impact Assessments and Responsible Divestment Plan for Business Region Eurasia, prepared by BSR as part of HRIAs for the company’s subsidiaries in Azerbaijan, Georgia, Kazakhstan, Moldova, Tajikistan, and Uzbekistan.¹³ In September 2015, Telia Company announced its intention to reduce its presence in Eurasia by divesting its Region Eurasia businesses. For this reason, BSR made recommendations in two distinct categories: a) For Telia Company, recommendations for how to integrate human rights into the sales process through a responsible divestment plan; and b) For each subsidiary and its current and future owners, recommendations for how to manage and mitigate human rights impacts during the ongoing management of the companies.</p> <p>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. The index determines risk scores on the basis of indicators that take into account freedom of expression and the unique characteristics of Orange’s business, such as the number of customers and employees in each market.</p> <p>Nokia was the first telecommunications vendor to define and to implement a human rights due diligence process to cover the sales of its products. The company uses this process to identify potential risks for product misuse and to investigate ways to mitigate these risks. In case a high risk is identified which cannot be mitigated, the company may decline the sale. To ensure all relevant cases are handled accordingly, flagging of the potential 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. Nokia finalized an extensive review of the due diligence process for its Networks business in December 2014, and the company is currently updating the process to improve it further.</p> <p>In 2012, Telefónica performed an assessment – following the framework offered by the Guiding Principles on Business and</p>

¹³ <http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/bsr-telia-company-hria-summary.pdf>.



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>Human Rights, and with the support of Business for Social Responsibility – within all its operations in order to evaluate the global impact of its activities. In 2014, Telefónica continued integrating the results of the assessment on the impact on Human Rights that was carried out in 2012 via its business units. This included a new evaluation to assess on a global scale how its operating businesses respond to governmental requests for users' personal data or content restriction, as well as the circumstances and contexts in which these petitions are generally received. As part of this process, in 2015, Telefónica will develop a global procedure guide regarding governmental requirements.</p>
<p>3. Create operational processes and routines to evaluate and handle government requests that may have an impact on freedom of expression and privacy.</p>	<p>At AT&T, such requests are evaluated by employees (including AT&T lawyers and, where necessary, local counsel familiar with applicable law) who are trained to confirm that requests are duly issued by an appropriate entity, under valid legal authority and are otherwise in compliance with applicable requirements. The company rejects government demands that do not satisfy these requirements. Where appropriate, it will seek clarification or modification of a request or object to a government demand or court order in the appropriate forum. These efforts help minimize the potential impact that government requests may have on AT&T customers' privacy and on their ability to communicate and access information of their choice.</p> <p>The Millicom Group Guideline for Law Enforcement Assistance Requests (LEA Guideline) was finalized and approved by their cross-functional Lawful Interception Policy Committee (LIP Committee) in Q1 2015. It clearly outlines our obligations within international frameworks, the roles and responsibilities of each department, assessments to be conducted as requests are received, how to handle urgent and non-written requests, how to log requests and our responses, how to protect customer data throughout the process of retrieving information, and how to deliver the information safely. A shortened version of this guideline is available publicly. Two controls relating to the implementation of the LEA Guideline were added in the Millicom Internal Control Manual in 2015. The first is to check that all requests are assessed by the legal team before execution and that a written copy of the original request is retained on file. The second control relates to</p>



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>limiting and making a log of access to customer data when executing the request. First controls were carried out in 2015. A 'Major events' Guideline was approved by the LIP Committee in Q3 2015. It defines steps to take in the case of a 'major event' and escalation process to regional and global levels. The Guideline also provides practical suggestions on how to engage with the authorities so as to limit the scope and/or timeframe of any 'major event'. Due to the sensitive nature of this document, it is not publicly available, but Millicom has presented its contents in meetings with Industry Dialogue and GNI.</p> <p>Telefónica has various processes in place to attend to requests made by local/governmental authorities. These processes are the responsibility of the General Secretary and Security of each of the Group's companies. The Privacy Committee and the Security Committee endeavor to sensitize and inform on the necessity to document such processes.</p>
<p>4. Adopt, where feasible, strategies to anticipate, respond and minimise the potential impact on freedom of expression and privacy in the event that a government demand or request is received that is unlawful or where governments are believed to be misusing products or technology for illegitimate purposes.</p>	<p>In one of its African markets, Millicom received a request to block a Web site considered by local authorities to present a threat to national security. The original blocking request did not fulfill the requirements for a lawful request, as it did not clearly originate from the competent authority. While the request itself followed local law, Millicom only acted on the request once the official format and process had been followed. This delayed the action by two days.</p> <p>In one of its African markets on June 1, 2014, government authorities contacted Orange by telephone and requested that it suspend SMS services throughout the country. In order to verify the legal basis for this request, Orange asked that the order be submitted in writing. On the following day, the country's four telecommunications operators received a written order, which cited the pertinent law, was signed by the authority with jurisdiction, and indicated that sanctions could result from noncompliance. The order was subsequently published in a pan-African newspaper. The companies complied with the order, resulting in the suspension of SMS services until July 24. The company learned several lessons as a result of this event, including the importance of cooperation among peer companies in responding to government demands that present irregularities, and that transparency can</p>



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>aid a company in responding to these demands.</p> <p>Telenor Group typically seeks to be transparent when possible, and communicates with customers and stakeholders e.g. through customer service, notices on its website, and public statements. 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. However, Telenor’s stance is to be transparent and this is communicated to relevant authorities. The company also engages actively with relevant authorities, seeking clarification e.g. on legal basis and timelines. Further, Telenor Group discusses with peers (both locally and within the Industry Dialogue), and has conversations with other stakeholders (locally and internationally). When needed, they also engage diplomatic channels and international organizations. They recognize that they will not always succeed using these tools, and may not be able to effectively impact the situation. There is a clear need to engage in longer-term dialogue, and not only when an incident occurs. The company has seen that awareness, interest and understanding for the challenges arising from authority requests needs to be built amongst authorities, other companies, organizations and stakeholders. They believe the stakeholder conversations of the Industry Dialogue and GNI are important in this regard.</p>
<p>5. Always seek to ensure the safety and liberty of company personnel who may be placed at risk.</p>	<p>The policies or practices of all participating companies reflect this Principle, and more details can be found by following links to individual companies’ reports on the ID Web site.</p> <p>Vodafone’s Code of Conduct includes a high-level commitment to protect the health, safety and well-being of its employees.¹⁴ The Global Policy Standard on Law Enforcement Assistance requires potential personal risk to individuals to be considered in any decision to challenge law enforcement demands.</p> <p>This general principle of the Orange Group prevails in all of its actions, particularly in the Central African Republic in 2014. Thus, the ministerial order to suspend the SMS networks, signed by the country's highest government authorities, duly</p>

¹⁴ See <http://www.vodafone.com/content/index/about/about-us/code-of-conduct.html>.



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>established by legal texts and the use of national security, was accompanied by the threat of personal sanctions in case of non-compliance. Orange, like other operators, therefore had to comply with the orders.</p> <p>Health, security, and occupational well-being are the three pillars of Telefónica, not only guaranteeing the protection of employees, but also to having a direct influence on their job satisfaction at the Company. Regarding physical security, the Global Security Directorate has established a series of guidelines to be followed, adapted to the risks identified for each country, as well as to cover the displacement process.</p>
<p>6. Raise awareness and train relevant employees in related policies and processes.</p>	<p>Vodafone's Global Policy Standard on Law Enforcement Assistance includes a requirement on training and awareness. In 2014/15, Vodafone rolled out a global e-learning course on Privacy and Human Rights. The course is designed for those who make decisions about government and law enforcement requests, but is available to employees in almost all markets. By the end of March 2015, it had been completed by more than 12,000 employees worldwide.</p> <p>Nokia focuses on training the teams directly involved in the due diligence process but have also included an introduction to the Human Rights Policy in the annual Ethical Business Training, which is mandatory for everyone working at Nokia. In 2015, Nokia conducted in-depth human rights training for selected key teams, covering areas such as prevention of product misuse, child labor, and forced labor. The target groups included senior management as well as customer teams, procurement, product management, and human resources teams in several countries across three different regions.</p> <p>AT&T's Privacy Policy provides detailed information about the customer information we collect, and how the company collects, stores and uses that information.¹⁵ Employees are required to complete compliance training, including privacy and data protection requirements, on a yearly basis. AT&T's Code of Business Conduct addresses company and individual employee commitments to protect the privacy of sensitive</p>

¹⁵ See http://about.att.com/sites/privacy_policy.



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>customer information and to comply with applicable laws and regulations of the countries where AT&T operates. All AT&T employees are trained on, and must acknowledge, the Code of Business Conduct on an annual basis; company officers receive in-person training on the Code. Finally, AT&T’s Human Rights in Communications Policy is available to all employees on the Sustainability website.</p>
<p>7. Share knowledge and insights, where relevant, with all relevant and interested stakeholders to improve understanding of the applicable legal framework and the effectiveness of these principles in practice, and to provide support for the implementation and further development of the principles.</p>	<p>Telefónica has undertaken a project to map local stakeholders for whom freedom of expression and privacy are key issues. The company will then use this data to determine how to engage with different stakeholders and improve the company’s responsiveness to stakeholder inquiries.</p> <p>Telia Company has also made publicly available its internal tool for assessments and escalation of government requests and demands with potentially serious impacts on freedom of expression in telecommunications.¹⁶ The document was initially shared with the other ID participating companies and with GNI in February 2015. A link to this form has been included in the GSMA policy handbook section on service restriction orders. The aim in sharing this tool is to support implementation and further development of industry best practice globally to promote and respect freedom of expression in telecommunications.</p> <p>Telenor Group collaborated with the Institute for Business & Human Rights to publish a case study on mobile network shutdowns.¹⁷ The study examines the impact of shutdowns on human rights in Pakistan, focuses on the efforts of Telenor Pakistan to use dialogue as a tool for reducing shutdown frequency and scope, and presents recommendations for both operators and governments.</p>

¹⁶ See <http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/template-foe-assessment-and-escalation-oct2016.pdf>.

¹⁷ See <http://www.ihrb.org/publications/reports/digital-dangers-case-study-pakistan.html>.



Guiding Principle	Examples of Industry Dialogue Implementation
<p>8. Report externally on an annual basis, and whenever circumstances make it relevant, on their progress in implementing the principles, and on major events occurring in this regard.</p>	<p>All of the ID companies have reported on their implementation of the ID Guiding Principles.¹⁸ Four ID companies have also published information about specific situations constituting major events as part of these reports or as news items on their company websites. Furthermore, ID operators AT&T, Millicom, Orange, Telenor Group, Telia Company, and Vodafone Group regularly publish reports that disclose statistics on the number of law enforcement requests they have received for customer data in certain countries or regions.¹⁹ ID companies have dedicated several shared learning sessions to the topic of transparency, but their different operating environments mean that each company takes a different approach to producing these reports.</p> <p>Millicom calls requests falling outside of normal law enforcement assistance requests ‘major events’. All local operations are required to escalate these events to global management and take a number of steps in order to minimize the effect of such events on our services. ‘Major events’ can include requests for shutdown of specific base station sites, geographical areas or entire network, service denial or restriction (SMS, mobile/fixed internet, social media channels), interception requests outside of due process, targeted take-down or blocking of specific content, denial of access for specific individuals, significant changes relating to surveillance techniques or operational processes (direct access or how local surveillance laws are implemented in practice), significant changes to local laws relating to government powers of surveillance or data retention, or requests to send politically motivated messages to customers on behalf of the</p>

¹⁸ See <http://www.telecomindustrydialogue.org/about/guiding-principles/>.

¹⁹ AT&T Transparency Report available at <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>; Millicom Law Enforcement Disclosure Report available at http://www.millicom.com/media/4562097/millicom_tr_law_2016_final_300316.pdf; Orange Transparency Report available at <http://www.orange.com/en/content/download/31105/933231/version/3/file/Orange+2014+transparenc+y+report.pdf>; Telenor Group Authority Requests Disclosure Report available at https://www.telenor.com/wp-content/uploads/2015/05/Authority-Requests-Disclosure-Report-2015_04.pdf; Telia Company Law Enforcement Disclosure Report available at http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/ledr_oct2016_final.pdf; Vodafone Law Enforcement Disclosure Report available at http://www.vodafone.com/content/index/about/sustainability/law_enforcement.html.



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>government. In 2015, a total of 20 events falling into the definition of 'major events' were reported to headquarters from the local operations. Five of these were events carried on from 2014. Fourteen of the events were in Africa.</p> <p>Telia Company has started to report publicly on unconventional requests and demands with potentially serious impacts on the right to freedom of expression. Telia Company aims to report on such events as they occur but also, as such communication is often not possible due to confidentiality provisions, to add some further information on such 'major events' in its biannual Transparency Reports. Telia Company has promoted freedom of expression by applying a practical point-of-challenge, most often by being transparent but also by requesting a government request be put in writing or postponing implementation inasmuch as the law allows, lobbying legislative initiatives and requesting blocking decisions to be put in writing. On those occasions when Telia Company was required to suspend services, the company did not state that this was the result of technical problems.</p> <p>Telenor Group reports annually on its sustainability performance in the sustainability section of their Annual Report and on their website. With respect to major events, the company seeks to be transparent, and when they can, share information with customers, post notes on their website or issues public statements.</p> <p>Telefónica Group reports its progress regarding the ID guiding principles for privacy and freedom of expression on an annual basis.²⁰</p>
<p>9. Help to inform the development of policy and regulations to support freedom of expression and privacy, including, alone or in cooperation with other entities, using its leverage to seek to mitigate potential negative impacts from policies or regulations.</p>	<p>The Industry Dialogue contributes to dialogue on the development of policy and regulations at both the national and international level. In addition to previous engagement with the Special Rapporteur, the Industry Dialogue has contributed comments to the following publications and projects:</p> <ul style="list-style-type: none"> • European Commission Guidance for the ICT Sector on implementing the UN Guiding Principles on Business

²⁰ <https://www.telefonica.com/en/web/sustainability/sustainability-reports/2014>.



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>and Human Rights²¹</p> <ul style="list-style-type: none"> • Council of Europe multi-stakeholder consultations on a Guide on Human Rights for Internet Users²² • The report of the UN High Commissioner for Human Rights on The Right to Privacy in the Digital Age²³ • Ranking Digital Rights²⁴ • The African Declaration for Internet Rights and Freedoms²⁵ • European Parliament Hearing on Human Rights and Technologies: the impact of digital surveillance and intrusion systems on human rights in third countries²⁶ • The World Bank Group’s review of its Environmental and Social Framework²⁷ • Australian Government Draft Guidelines for the blocking of websites²⁸ <p>In July of 2014, the ID published a statement outlining its commitment to respect user privacy.²⁹ For the Industry Dialogue, intrusions on the right to privacy should meet the requirements of legality, necessity, and proportionality that have been established in international human rights law. The ID expressed the view that government surveillance programs should be subject to ongoing review by an independent authority and that governments should not conduct any type of registry, search, or surveillance by means of direct access to companies’ infrastructure without any technical control by the company or without the company controlling the scope of the data collection. This statement has guided the Industry</p>

²¹ <http://www.ihrb.org/pdf/eu-sector-guidance/ICT/The-Telecommunications-Industry-Dialogue.pdf>.

²² <http://www.telecomindustrydialogue.org/wp-content/uploads/ID-Comments-COE-Guide-HR-Internet-Users-Nov-2013.pdf>.

²³ <http://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Dialogue-input-OHCHR-1-April-2014.pdf>.

²⁴ <http://www.telecomindustrydialogue.org/wp-content/uploads/ID-comments-RDR-Phase-1-V2.pdf>.

²⁵ <http://www.telecomindustrydialogue.org/wp-content/uploads/ID-Comments-to-African-Declaration-Aug-2014.pdf>.

²⁶ <http://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Dialogue-submission-Human-Rights-Tech-hearing.pdf>.

²⁷ <http://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Dialogue-submission-World-Bank-11-Feb-2015.pdf>.

²⁸ <http://www.telecomindustrydialogue.org/wp-content/uploads/ID-Input-to-Australian-Guidelines-3.pdf>.

²⁹ <http://www.telecomindustrydialogue.org/wp-content/uploads/IDCommitmentUserPrivacy20141.pdf>.



Guiding Principle	Examples of Industry Dialogue Implementation
	Dialogue in its conversations with government authorities and its inputs to public consultations on matters involving the Principles.
10. Examine, as a group, options for implementing relevant grievance mechanisms, as outlined in Principle 31 of the UN Guiding Principles for Business and Human Rights.	Since its inception in 2013, the Industry Dialogue has devoted four learning sessions on the subject of grievance mechanisms and remedy. The group has examined research and reports on this topic by organizations such as Shift, the Institute for Human Rights and Business, CSR Europe, Access Now, and the International Federation for Human Rights (FIDH). Additionally, in February 2015, the OECD's Responsible Business Conduct Unit held a learning call with the Industry Dialogue, and its experts described the specific instances procedure and answered questions from participating companies. Our learning sessions have revealed that every Industry Dialogue company has a mechanism by which employees and customers can submit complaints. Escalation procedures are generally in place to ensure that representatives of the legal, compliance, and sustainability teams are notified about certain complaints and can participate in resolving them. Some company forms for filing complaints specifically provide the option of raising human rights issues, and ID Board members may be notified when such complaints are filed. Some companies also provide the names and contact details of staff members responsible for corporate social responsibility on their Web sites. ID companies seldom receive formal complaints related to freedom of expression and privacy. When such a demand does come, the Principles provide that companies can seek to minimize the impact on customers' rights by, for example, reviewing the demand with the relevant authority to seek clarification or modification, seeking judicial review where available, and engaging with other stakeholders in support of freedom of expression and privacy. ID Principle 8 also indicates that companies will report externally on major events as appropriate. ID companies will continue to accept complaints related to freedom of expression and privacy through their existing mechanisms. They will generally seek to ensure that these are consistent with the effectiveness criteria established in UN Guiding Principle 31 and that actions that



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>serve as reparations are informed by international human rights instruments.³⁰ At the same time, it may be constructive to approach grievance and remedy in the ICT sector in broader terms. The Industry Dialogue has identified a few good practices in this regard:</p> <ol style="list-style-type: none">1) Telecommunications companies should ensure that they have a procedure for handling both complaints and major events that involve human rights.2) When a major event requires the shutdown of a communications service or restriction of content, companies should attempt to minimize the duration or scope of the request and restore access to the service or content as soon as possible where this is feasible, as a means of restitution (this is generally in the company's commercial interest as well).3) Companies should aim to be transparent with the public about major events that impact the freedom of expression and privacy of their customers and users, as outlined in ID Principle 8. Currently, ID companies achieve this through their annual reporting on corporate social responsibility, law enforcement disclosure reports, news releases about specific events, communications with customers (e.g. via customer care representatives or other channels for customer communication), and dialogue with stakeholders who may represent the interests of affected users, such as civil society organizations or media outlets. These actions may constitute a means of satisfaction.4) Companies can incorporate the lessons learned from challenging situations into company policies and procedures, training material for employees, and policy advocacy with governments. These steps may equate guarantees of non-repetition.

³⁰ Reparations in human rights law are generally governed by the principles of restitution, compensation, rehabilitation, satisfaction, and guarantees of non-repetition, as outlined in, e.g., Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, adopted by General Assembly Resolution 60/147 of 16 December 2005.



Guiding Principle	Examples of Industry Dialogue Implementation
	<p>Some civil society organizations have called on telecommunications operators to provide compensation to customers affected by the shutdown of communications services or government demands for user data. For operators, this presents serious challenges for several reasons. First, limitations on customer freedom of expression and privacy typically result from government demands under applicable domestic laws. Companies must abide by the laws of the jurisdictions where they operate; they may not pick and choose which laws to follow. Refusal to comply with laws would have serious consequences for telecommunications operators and for their employees in a country, and may raise other concerns relating to the duty of corporations to respect local law. In recognition of this, the ID Principles suggest that companies attempt to modify or challenge problematic demands and work with governments to make their laws more protective of freedom of expression and privacy. Second, in the context of communications service shutdowns, telecommunications operators lose revenue when they must suspend services in response to government demands. Governments do not compensate operators for these losses. An approach that would require companies to incur a further penalty when service shutdowns occur would likely discourage responsible companies from conducting business in challenging markets. Finally, as a practical matter, in some of the markets where shutdowns frequently occur, the majority of customers have prepaid contracts, adding an extra layer of complexity to any reparations regime. These points have emerged from our discussions on grievance and remedy thus far. We welcome the opportunity to explore this topic further with those engaged in research and advocacy on the subject.</p>

Conclusion

The Industry Dialogue welcomes this opportunity to share information about concerning trends across the legal frameworks that impact freedom of expression in telecommunications, as well as the good practices that have emerged through implementation of the Guiding Principles across our companies. We recommend that this report highlight the critical importance of clear laws that meet international human



rights standards, and which provide an enabling environment in which Telcos can demonstrate their respect for freedom of expression and privacy rights. Laws that concern freedom of expression and privacy in the ICT sector should be accompanied by clear procedures and processes for implementation, and should be subject to independent, effective oversight mechanisms which are properly resourced. We encourage states to adopt laws and policies that require transparency and accountability by governments and permit transparency by companies, and encourage governments, companies, and key stakeholders from around the world to work together to further this discussion.

Thank you for the opportunity to present our submission.

Sincerely,

Laura Okkonen
Nokia Group
Chair of the Telecommunications Industry Dialogue