The GNI Principles at Work

PUBLIC REPORT ON THE THIRD CYCLE OF INDEPENDENT ASSESSMENTS OF GNI COMPANY MEMBERS 2018/2019

GLOBAL NETWORK INITIATIVE

Global Network Initiative

The GNI **Principles at Work**

Public Report on the Third Cycle of Independent Assessments of GNI Company Members

2018/2019

Follow Us

Twitter: @theGNI
Facebook: #theGNI

Contact Us

718 7th Street NW
Washington DC 20001
202-793-3053
info@globalnetworkinitiative.org
globalnetworkinitiative.org

Table of Contents

Executive Summary

This is the public report on the 2018/2019 independent assessments of 11 member companies of the Global Network Initiative (GNI): Facebook, Google, Microsoft, Millicom, Nokia, Orange, Telefónica, Telenor Group, Telia Company, Verizon Media, and Vodafone Group. This assessment cycle covered a two-year period, from July 1, 2016, to July 1, 2018 ("the assessment period"). However, only for this assessment cycle, the relevant period of review for Millicom, Nokia, Orange, Telefónica, Telenor Group, Telia Company, and Vodafone Group spanned from their accession to GNI on March 27, 2017, to July 1, 2018.

GNI was launched in 2008. Its mission is to protect and advance freedom of expression and privacy rights in the information and communications technology (ICT) sector by setting a global standard for responsible decision making and serving as a multistakeholder voice in the face of government restrictions and demands. GNI brings together ICT companies, civil society (including human rights and press freedom groups), academics, academic institutions, and investors from around the world to provide a framework for responsible company decision making, foster accountability by member companies, offer a safe space for shared learning, and provide a forum for collective advocacy in support of laws and policies that promote and protect freedom of expression and privacy.

A unique feature of GNI is its independent assessment process that relies on a methodology designed to allow GNI's civil society, academic, and investor board members (non-company board members) insight into member company efforts to implement the GNI Principles on Freedom of Expression and Privacy ("the GNI Principles"). This report marks the third cycle of GNI company assessments. Based on a detailed evaluation of confidential reports prepared by independent assessors, and the querying of the assessors and member companies, GNI's multistakeholder Board of Directors reviewed the assessments and determined that each company is making good-faith efforts to implement the GNI Principles with improvement over time.

> "The assessment process strives to increase company transparency while protecting users' rights through ample access to information."
>
> **GARE SMITH,** Foley Hoag LLP

The independent assessments were conducted according to the GNI Assessment Toolkit by assessors accredited by the GNI Board as meeting independence and competency criteria established by GNI, who then participated in mandatory assessor training. Assessors received access to information, including relevant documents in secure settings. They also had access to key company personnel, from frontline teams to senior management, and conducted a total of 125 interviews. Assessments included an examination of 86 case studies, which looked at how the companies are dealing with government requests and demands in practice. The GNI Board met four times over the course of 2019 to review the 11 company reports

and engage in detailed discussion with each company and assessor before making their determinations.

The GNI assessment process is confidential by design. It allows companies to share and discuss sensitive cases of government requests with GNI's non-company board members. It also allows discussion of internal company systems and processes to implement the GNI Principles. This report primarily presents information in aggregate or anonymized form in order to show how the companies review and respond to government requests, without disclosing confidential or otherwise legally protected information. To increase transparency with the public, this report includes some examples of case studies and assessor recommendations specific to individual companies.

This report shares the findings from the 11 company assessments. Points of progress and areas for future shared learning identified in the report include further consideration of how companies integrate the GNI Principles into their business operations, ways to enhance and expand training efforts inside companies, and developing tools and guidance on topics such as human rights due diligence (HRDD) and impact assessment.

The assessments also provide insights into the external operating environment for companies. These include ongoing challenges around state surveillance and impediments to transparency, challenges responding to government-ordered network disruptions, and the need for greater collaboration with civil society and other stakeholders to engage governments to bring their laws and policies into alignment with international human rights norms.

This cycle of assessments provides a window into how a growing number of companies from across the ICT sector are exercising their responsibility to uphold the rule of law and respect the freedom of expression and privacy rights of billions of users and customers while dealing with increasingly sophisticated government measures to assert control over online content and digital communications.

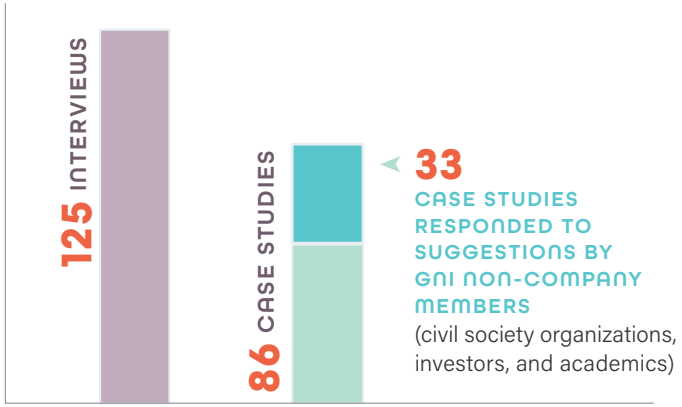
No single company can face today's freedom of expression and privacy challenges on its own. Pushing back on efforts to suppress freedom of expression and privacy rights or limit the operating environment for rights-respecting ICT companies requires dedicated efforts by governments, regulators, companies, and other key stakeholders, including investors, academics, and civil society organizations inside and outside of GNI.

The assessment process shows how companies from different segments of the ICT sector can commit to a common set of fundamental freedom of expression and privacy principles, grounded in international human rights law and commitments to accountability, collaboration, shared learning, and public policy. After the publication of this report, each company will communicate to the public about the outcome of its assessment.

Going forward, GNI will work to integrate insights from this assessment cycle into our wider efforts to protect and promote freedom of expression and privacy in the ICT sector. Specific steps will include:

- A complete review of the assessment process to strengthen our standards and practices for the fourth GNI assessment cycle,
- The integration of findings from the assessments into shared learning across and within constituencies, and
- Using insights from the assessment to inform and enhance GNI's collaborative engagement with governments on freedom of expression and privacy rights.

KEY NUMBERS OF THE THIRD ASSESSMENT CYCLE



9 COMPANY BOARD MEMBERS[1]

10 NON-COMPANY BOARD MEMBERS

[1] The GNI Governance Charter describes the composition of the board. There can be up to 10 company representatives. In cases where there are open board seats in a constituency group, the voting authority for those open seats shall be evenly distributed among representatives of that constituency group on the board.

1) Introduction

1) Introduction

About the Global Network Initiative

This is the public report on the third cycle of the Global Network Initiative (GNI) independent company assessment process.

GNI brings together companies, civil society organizations, investors, and academics to enhance freedom of expression and privacy in the information and communications technology (ICT) sector. By committing to the GNI Principles on Freedom of Expression and Privacy ("the GNI Principles"), our members work to actively promote and facilitate responsible company decision making and serve as a multistakeholder voice in the face of government restrictions and demands. Since it was launched in 2008, GNI has helped companies improve their policies and procedures, provided a forum for shared learning, and promoted collaborative policy engagement in support of freedom of expression and privacy rights. As of December 31, 2019, GNI had 64 members from 23 countries across Africa, Asia, Europe, Latin America, North America, and the Middle East, including the companies assessed during this cycle serving billions of users worldwide. Visit GNI's website and watch this video to learn more.

About the Assessment Process

Companies participating in GNI are independently assessed periodically on their progress in implementing the GNI Principles. The purpose of the assessment is to enable the GNI Board to determine whether each member company is "making good-faith efforts to implement the GNI Principles with improvement over time" during the period covered by the assessment.[2]

The GNI Principles are grounded in international human rights law and informed by the corporate responsibility to respect human rights articulated in the UN Guiding Principles on

GNI IN THE ICT SECTOR ACCOUNTABILITY ECOSYSTEM

The GNI Principles are rooted in the rule of law and internationally recognized laws and standards for human rights. GNI was founded to address the gap that can arise in this system, when governments use national laws to compel ICT companies to take actions that infringe upon the freedom of expression and privacy rights of users. As a multistakeholder initiative, GNI's core commitments complement the national laws and regulations that affect ICT sector companies, including consumer privacy and data protection regulations. In this regard, GNI should be viewed as one component of a wider ecosystem of accountability for ICT companies around the world.

[2] For the four previously assessed companies, the assessment period was from July 1, 2016, to July 1, 2018. Only for this assessment cycle, the relevant period of review for Millicom, Nokia, Orange, Telefónica, Telenor Group, Telia Company, and Vodafone Group spanned from their accession to GNI from March 27, 2017 to July 1, 2018.

Business and Human Rights (UNGPs).[3] The GNI Principles state the overarching commitment of members to collaborate in the advancement of user rights to freedom of expression and privacy in the context of government demands. The GNI Implementation Guidelines provide more detailed guidance to ICT companies on how to put the GNI Principles into practice, and also provide the framework for collaboration among companies, NGOs, investors, and academics.

Commitment to the GNI Principles has had a meaningful impact on ICT companies' practices, as reported by the Ranking Digital Rights (RDR) Corporate Accountability Index:[4]

"As in previous iterations of the RDR Index, the top governance scores this year all went to companies that are members of GNI, a multistakeholder organization that focuses on upholding principles of freedom of expression and privacy, primarily in relation to government requests."[5]

An independent company assessment includes both a company process review and a review of specific case studies:

- The process review examines a company's systems, policies, and procedures to implement the GNI Principles.
- The case studies assess a number of specific cases for each company in order to show whether and how the company implemented the GNI Principles in practice.

The 2018/2019 independent company assessment cycle included 11 companies — the largest number thus far — including telecommunications network operators, and an equipment vendor.

[3] Specifically, the GNI Principles are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR"). The application of these Principles is informed by the UN Guiding Principles on Business and Human Rights ("UN Guiding Principles"), the 'Protect, Respect, and Remedy' Framework and the OECD Guidelines for Multinational Enterprises.

[4] Not all GNI member companies are ranked by Ranking Digital Rights.

[5] 2019 RDR Corporate Accountability Index, p. 25.

GNI ASSESSMENT CYCLES AT A GLANCE

ASSESSMENT CYCLE	NUMBER OF COMPANIES ASSESSED	NUMBER OF INTERNET SERVICES COMPANIES	NUMBER OF TELECOMMUNICATIONS COMPANIES	NUMBER OF EQUIPMENT VENDORS	NUMBER OF ACCREDITED ASSESSORS
2013/2014	3	3	0	0	5
2015/2016	5	5	0	0	7
2018/2019	11	4	6	1	12

Prior to the assessments, GNI developed the Assessment Toolkit, a comprehensive overview of the assessment methodology. This effort to make the assessment process more transparent and efficient is the result of revising the Assessment Guidance and Reporting Framework documents,[6] processing the lessons and recommendations from past assessment cycles and studying best practices from various public reporting standards.[7]

Only organizations accredited by the multistakeholder GNI Board are eligible to conduct independent assessments of member companies. Accredited assessors must meet the independence and competency criteria required by GNI, which include meeting the highest professional standards and maintaining independence from the companies they assess.

In September 2018, at the outset of this assessment cycle, GNI delivered a training to all 12 accredited assessors. The training reviewed the GNI Principles and Implementation Guidelines, discussed how GNI's assessment process relates to the assurance of sustainability reporting of some companies, and introduced the Assessment Toolkit. See the Assessment Q&A and Step-by-Step Guide to learn more.

Accountability, Transparency, and Confidentiality

The GNI Principles state: "Participants will be held accountable through a system of (a) transparency with the public and (b) independent assessment and evaluation of the implementation of these Principles."

"The process of implementing the GNI Principles has helped us to strengthen the governance and internal awareness around digital rights, thus contributing to our common goal of promoting privacy and freedom of expression."

GEERT PAEMEN, Telefónica

GNI companies have continuously innovated and improved on their commitment to public transparency. The information presented in this report supplements other publicly available information about company conduct. The assessment process is confidential by design, involving the details of sensitive cases of government requests and confidential company systems, policies, and procedures. Strict confidentiality allows GNI Board members from civil society, academia, investors, and other companies to gain insights and provide feedback that would not otherwise be possible in an open process.

"The confidentiality of the assessment process — and the mutual trust it is built on — supports a completely unique and collaborative environment within the GNI. During assessments, academics like myself as well as civil society organizations and socially responsible investors engage with the thorniest challenges that our company members face in protecting user free expression

6 The Assessment Guidance and Reporting Framework are documents that described the methodology for previous assessments.

7 The Toolkit draws from the Global Reporting Initiative (GRI) and the UN Guiding Principles Reporting Framework. See also GNI Assessment Toolkit, p. 3.

and privacy. The case study section of the Assessment Toolkit gives us opportunities to dig deep into particular situations, understand the competing pressures that tech and telco companies face, and provide input in line with the GNI Implementation Guidelines. It's challenging, even exhausting, work, but over time I think this engagement has a real impact on the tech sector's preparedness to defend its users' human rights."

JESSICA FJELD, Berkman Klein Center for Internet & Society at Harvard University

This report provides a summary of the independent assessments of all 11 companies. The majority of the case studies are anonymized, and data and recommendations are aggregated to provide key learning points without compromising security and confidentiality.[8] Where appropriate, some examples and cases have been attributed to specific companies. The report also aims to provide an overview and some reflections on key developments that are influencing or impacting the ICT sector as a whole in relation to freedom of expression and privacy rights, as illustrated by this cycle of company assessments.

[8] For example, the GNI Principles state: "Participating companies, when implementing these Principles, will always seek to ensure the safety and liberty of company personnel who may be placed at risk."

2) 2018/2019 Assessments

2) 2018/2019 Assessments

ASSESSED COMPANIES

The following GNI member companies were independently assessed during the 2018/2019 assessment cycle:

COMPANY	TYPE	ASSESSMENTS COMPLETED	CASES REVIEWED '18/'19
Facebook	Internet	2	8
Google	Internet	3	9
Microsoft	Internet	3	9
Millicom	Telecommunications Operator	1	6
Nokia	Equipment Vendor	1	7
Orange	Telecommunications Operator	1	8
Telefónica	Telecommunications Operator	1	8
Telenor Group	Telecommunications Operator	1	7
Telia Company	Telecommunications Operator	1	8
Verizon Media[9]	Internet	3	8
Vodafone Group	Telecommunications Operator	1	8

[9] In June 2017, Yahoo, a founding member of GNI, was acquired by Verizon and joined with AOL to form Oath. In January 2019, Oath re-branded as Verizon Media.

ASSESSORS

From the pool of accredited assessors, the following organizations were selected by the 11 companies to conduct the assessments described in this report:

Deloitte Denmark[10]

DNV GL

Foley Hoag LLP

KPMG Asesores SL

KPMG AG (Switzerland)

Osborne Clarke

SSP Blue

[10] Deloitte Denmark worked with teams from Deloitte Spain and Deloitte Sweden to conduct the assessments.

Assessor Access to Information

As required by the Assessment Toolkit, each assessor stated in their report whether they had sufficient access to information to conduct the assessment and provided details on the nature of the information to which they had access, including documents and interviews.[11] For all of the assessed companies, the assessors informed the GNI Board that they had sufficient access to information to effectively conduct the assessment. When they were unable to review specific documents or access certain information due to limits on disclosure, they were able to make use of alternative approaches that were sufficient to acquire the necessary information. These approaches included interviews with senior management and other relevant employees, reviewing written responses to specific questions, reading secure documents on screens of company personnel, and examining documentation of incoming government requests and outgoing company responses.

"As an assessor, we were able to really dive into how a company analyzes and handles human rights issues in their risk management processes. This gave us a sound basis for assessing their progress in implementing the GNI Principles."

HELENA BARTON, Deloitte

[11] Per the Assessment Toolkit, "GNI recognizes that legal requirements may bar companies from disclosing information that is otherwise relevant to the assessment process. GNI further recognizes that companies may not be able to disclose other relevant information to protect attorney-client privilege, to maintain user privacy, to fulfill its contractual commitments, or for competitive reasons, including to comply with antitrust laws. Each company will be required to identify limitations on access to information, if any, to the assessor with as much specificity as is practicable."

LIMITS ON DISCLOSURE

The GNI assessments are a review by independent third-party assessors of company responses to government requests implicating freedom of expression and privacy. Both external and internal company constraints limit the information available to assessors. In addition to the concerns noted above regarding the personal safety of company employees, there are additional limits on disclosure. These limits were recognized at the time of the formation of the GNI. Specific reasons for limits on disclosure include the following:

Legal Prohibitions

There are situations where companies are legally prohibited from disclosing information. For example, in the United States, some companies face non-disclosure obligations covering National Security Letters and United States Foreign Intelligence Surveillance Act (FISA) orders.

User Privacy

Companies have legal obligations to maintain the privacy of users' personal information as set out in their privacy policies and Terms of Service. This can affect a company's ability to disclose information about a case, even if that case is well known and has been the subject of public reporting.

Attorney-client Privilege

These are instances where internal company information is provided to an attorney in the course of seeking legal advice, and there are limits on disclosure for both this information and the legal advice received from such attorney.

Company Confidential Information / Trade Secrets

GNI assessment reports are reviewed by the GNI Board, which includes representatives from other GNI member companies. Companies may withhold confidential information from the assessment process, whether to protect trade secrets, or out of other concerns, such as compliance with applicable antitrust and competition laws. An antitrust review is completed on the assessment reports by a law firm prior to their distribution to the GNI Board.

Assessor Findings

This section presents key findings from across the company assessment reports, noting common aspects and approaches to implementing the GNI Principles. This section also includes a set of individual cases that have been anonymized by company, and in some cases also by country. It draws directly from assessment reports presented to the GNI Board. While there are many common elements to those reports, the reports were of varying quality, length and detail, and the board considered each report independently.

THE ROLE OF THE ASSESSOR AND THE GNI BOARD

It is the role of the GNI Board — and not of the independent assessor — to determine whether a company is making good-faith efforts to implement the GNI Principles with improvement over time during the assessment period. The role of the independent assessor is to provide the board with the information it needs to make this determination. The board considers the company's record during the assessment period on implementing the GNI Principles as it makes this determination.[12]

[12] According to the GNI Independence and Competency Criteria: "For independent assessment, an important role of the assessors is to provide information on the performance of the company in implementing GNI's Principles to GNI's Board. This will require the assessors to provide substantive commentary on the performance of the company against GNI's Principles and Implementation Guidelines as set out in the GNI Assessment Toolkit. It is the role of the GNI Board to determine whether a company is making good-faith efforts to implement the GNI Principles with improvement over time during the period covered by the assessment. This determination will be heavily influenced by the results of the independent assessors' work. This will require assessors to commit to reporting to GNI's Board as detailed in the reporting template, in a format which will provide adequate information, analysis, conclusions, and recommendations for the GNI Board to be able to make a determination." More information on the role of the board is provided in Section 4 of the Assessment Toolkit.

Process Review

The process review consisted of a series of questions about the systems, policies, and procedures that companies use to implement the GNI Principles. Below we report on findings common to the 11 assessed companies from each of the categories covered in the process review. The individual company determinations provide more information about unique and noteworthy aspects of each company's approach as detailed in the assessment reports. It is important to note that the implementation of the GNI Principles is not a one-size-fits-all exercise, and that the policies and processes examined during the assessment process are applied in a wide range of contexts, from routine matters to highly complex and sensitive situations. The below summary of common elements from the process review should be read in conjunction with the case studies, which aim to provide a sense of this wide variation across different contexts.

"As an investor that has worked with the GNI independent assessment process since its inception, I have always been painfully aware of the tension between external stakeholders' need to know and the confidentiality of our process. We've made real strides in opening up the process to the outside world, and we'll continue to do so. But it is important to understand why the integrity of the process depends upon confidentiality. It is built on a foundation of good faith and trust. Companies spend substantial

time and resources to undergo this voluntary process because they see value in it. They share the details of some very difficult decisions because they respect the process and want feedback and guidance from the GNI's multistakeholder board. It would simply be impossible to maintain this degree of trust in an open environment. Any evaluation process that seeks to promote 'improvement over time' must provide a safe space to discuss the hardest challenges."

ADAM KANZER, BNP Paribas Asset Management

Governance

Each of the assessment reports described the company's governance structures for implementing the GNI Principles. These structures vary significantly, but all included:

- A senior-directed human rights function within the company.
- The board or one of its subcommittees receiving and evaluating reports from senior management on human rights issues, including freedom of expression and privacy.
- Personnel training on freedom of expression and privacy risks, with varying approaches (see the Lessons and Opportunities Section of this report).
- Processes to evaluate and, where appropriate, escalate freedom of expression and privacy issues to higher levels in the company. For example, see Telia Company's escalation form and Millicom's Law Enforcement Assistance and Major Events Policy.

Due Diligence and Risk Management

Each assessment report described company processes and mechanisms to identify potential risks to freedom of expression and privacy connected to their operations, including products, markets, acquisitions and partnerships, and other business relationships. Each company had mechanisms to assess human rights impacts when due diligence identifies circumstances when freedom of expression and privacy may be jeopardized or advanced. Specific processes are discussed in greater detail below in each company determination and vary from integrating the assessment of human rights risks into broader company due diligence processes to performing specific human rights impact assessments (HRIAs). For example, see Verizon Media's approach to HRIAs. In addition, all of the companies had processes to prevent or mitigate risks identified by due diligence processes, with differing approaches when the company does and does not have operational control.

Freedom of Expression and Privacy in Practice

Each assessment report described the policies and procedures that set out how the company will assess and respond to government restrictions and demands for user information.[13] According to the reports, these processes call for:

- Governments to follow established domestic legal processes when they are seeking to restrict communications or access personal information.
- Clear, written communications from the government that explain the legal basis for government-mandated service restrictions and government demands for personal information.
- Narrow interpretation of government requests, including regarding the requesting government's jurisdiction, to minimize impacts on users.

13 One exception to this section is Nokia, which as a vendor company does not receive government orders to restrict content and turn over user data. See the Nokia Company Determination in this report for more about this issue.

- Where possible and legally permitted, detailed record keeping of all incoming government requests substantiating the legal basis for a restriction or demand, including records of verbal demands, which, in certain jurisdictions, are permitted by law in emergency situations. [14]

The processes also addressed how the company would respond when a government fails to provide a written directive or adhere to legal procedure.

Each assessment report described the policies and procedures a company has in place to respond to government restrictions or demands that appear overbroad,[15] unlawful, or otherwise inconsistent with domestic law or procedures or international human rights laws and standards on freedom of expression or privacy. In appropriate cases and circumstances, company policies and procedures enabled them to:

- Seek clarification or modification of government restrictions or demands that appear inconsistent with domestic or international law;
- Seek assistance from relevant government authorities, international human rights bodies, or non-governmental organizations when faced with such demands; and/or
- Challenge such demands in domestic courts.[16]

[14] Per application guidance in the GNI Implementation Guidelines: "Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written."

[15] Per application guidance in the GNI Implementation Guidelines: "Overbroad could mean, for example, where more information is restricted than would be reasonably expected based on the asserted purpose of the request."

[16] Per application guidance in the GNI Implementation Guidelines: "It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression and privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend."

Each assessment report also described company processes to engage with governments to encourage laws, regulations and restrictions, and demands that are consistent with international law and standards. These processes varied from company to company, but include responsibilities for government relations, regulatory affairs, or public policy teams to interact with legislators, regulators, and government officials to encourage consistency with human rights norms and that the rights to freedom of expression and privacy are respected.

Examples included:

- Microsoft's advocacy for principles for international agreements to govern law enforcement access to data and regulation of government use of facial recognition.
- Nokia's engagement with the Finnish Foreign Ministry with regards to human rights considerations around the export of certain products to certain countries, in some cases even regardless of whether these products are subject to formal export controls. Nokia has provided several Finnish government agencies with briefings regarding its implementation of the GNI Principles, its policies and procedures to carry out human rights due diligence prior to selling its products, and other business and human rights issues.
- Telia Company's Law Enforcement Disclosure Reporting, as well as Telia Company's series of articles on legislative initiatives and unconventional requests, aim to provide transparency to inform debates on freedom of expression and surveillance privacy.
- Telefónica's advocacy work around its "Manifesto for a New Digital Deal" to promote a human-centric digitalization, which has been presented in various countries to high-ranking representatives from government, the private sector, and civil society.

"With our Digital Manifesto, we are advocating for a human-centric digitalization through a modernization of our policies and with the aim to better defend people's rights and our shared values. Improving accountability through GNI´s assessment has helped us a lot in this process, it is key for our work."

CHRISTOPH STECK, Telefónica

The assessment reports also described company engagement through industry and multistakeholder initiatives. Examples of such initiatives, aside from GNI, include the Freedom Online Coalition Advisory Network, the GSM Association (GSMA), the European Telecommunications Network Operators (ETNO), and the Reform Government Surveillance (RGS) Coalition, among others.

Transparency and Engagement

Each assessment report described how companies:

- Communicated their general approach to addressing human rights impacts in relation to freedom of expression and privacy to shareholders and stakeholders. See the Company Determinations Section of this report for links to publicly available reports, websites, and other ways in which companies disclose this information, including:
  - The generally applicable laws and policies that require the company to restrict content or communications or provide personal information to government authorities.
  - The company's policies and procedures for responding to government restrictions and demands.
  - Published reports about the requests and demands that companies receive from governments.[17]
- Used a variety of means to communicate internally to their employees about their commitments to freedom of expression and privacy, including the GNI Principles.
- Engaged with government officials on reforms of laws, policies, and practices that infringe on freedom of expression and privacy through a variety of means, as shown in select case examples in this report.

Follow Up and Improvement

The GNI Board's standard of review is whether a company is making "good-faith efforts to implement the GNI Principles with improvement over time." See the Improvement Over Time Section of this report for an anonymized overview of recommendations presented to companies to consider, as well as actions taken by companies after considering recommendations from previous assessment cycles.

[17] One exception is Nokia, which as a vendor company does not receive government orders to restrict content and turn over user data. See the See the Nokia Company Determination in this report for more about this issue.

Case Studies

"Throughout the assessment process, we examined case studies discussing how companies apply the GNI Principles to respond to requests from governments to censor content, restrict access to communications services, or provide access to user data. The cases also offered important learning opportunities about the application of GNI Principles in different jurisdictions, even when the laws in place may limit transparency."

KYUNG SIN PARK, Korea University Law School

The review of Case Studies provides a window into whether and how companies are implementing the GNI Principles in practice. This section presents findings from the case studies in aggregate, as well as examples of cases, anonymized by company and/or country as necessary.

Over the assessment period, an individual company may receive thousands of individual government requests relating to freedom of expression or privacy. The GNI Board and the independent assessor can only review a small sample of these cases. Assessors select cases from those proposed by both GNI non-company members and by the company being assessed, according to a process described in the Assessment Toolkit.[18] These case studies are intended to illustrate various aspects of each company's processes, in practice, and to highlight particular challenges faced. The case studies reviewed do not represent a statistically significant sample of all cases handled by a given company, and therefore no inferences can be drawn about the total population of requests received by any company during the reporting period.

"While examining various cases, we were sure to include cases recommended by non-company participants as well those selected by our assessed company, and those as assessors we thought worthy of analysis. The breadth of the cases and the depth of review inspired by the GNI assessment process helped us delve deeply into the multiple challenges a company may face when protecting the right to freedom of expression and privacy in the online environment. It also allowed us to identify successes and recommended areas of improvement."

HEMANSHU NIGAM, SSP Blue

[18] See the GNI Case Selection Guidance Summary. For more on the role of the non-company constituencies in case selection, see Section 3.2 of the Assessment Toolkit.

OVERVIEW OF CASES

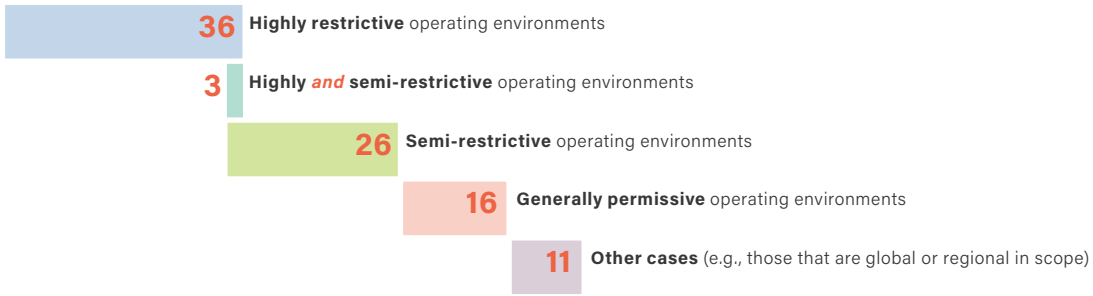
TOTAL NUMBER OF CASES REVIEWED: 86

A single case may cover multiple topics. For example, a particular government demand may impact both the free expression and privacy rights of a company's users. Similarly, a case may consist of a single instance or multiple sets of similar incidents. A case could also represent how a company operates in a particular environment, rather than how it responded to a specific government request. See Assessment Toolkit, p.7

CASES BY OPERATING ENVIRONMENT

CASES BY OPERATING ENVIRONMENT

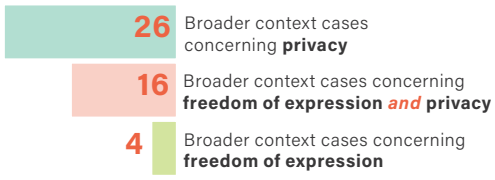
The Case Selection Guidance provided by GNI non-company members highlighted threats to freedom of expression and privacy across different operating environments. These operating environments are classified as highly restrictive, semi-restrictive, and generally permissive. The assessors and companies used this guidance as part of the case selection process.

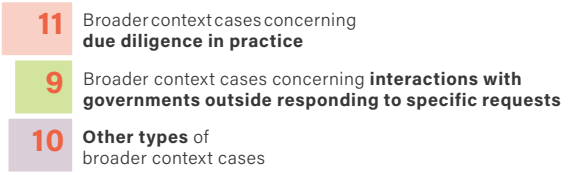


CASES BY TYPE

CASES INVOLVING A SPECIFIC GOVERNMENT REQUEST: 56

CASES RELATED TO THE BROADER CONTEXT OF COMPANY OPERATIONS: 30[19]





Examples of other types of broader context cases:

- Grievance mechanisms
- Transparency reporting about government restrictions and demands
- Updating policies and procedures
- Human rights impact assessments
- Litigation related to freedom of expression and privacy

[19] Cases about the broader context of company operations are about implementing the GNI Principles but are not about specific government requests and demands. They may look at how due diligence processes work in practice, company interactions with governments outside of responding to specific requests and demands, grievance mechanisms, or other topics.

CASES BY GEOGRAPHY

REGION	COUNTRIES[20]			NUMBER OF CASES
EAST ASIA & PACIFIC	China Myanmar	Indonesia Thailand	Malaysia Vietnam	13
EUROPE & CENTRAL ASIA	Belarus France Kazakhstan Turkey	Denmark Germany Spain Russia	Finland Italy Sweden United Kingdom	31
LATIN AMERICA & CARIBBEAN	Brazil Honduras	Colombia Paraguay	El Salvador Venezuela	10
MIDDLE EAST & NORTH AFRICA	Egypt Saudi Arabia	Israel	Palestine United Arab Emirates	6
NORTH AMERICA	Canada		United States of America	4
SOUTH ASIA	India		Pakistan	4
SUB-SAHARAN AFRICA	Cameroon Guinea		Chad Niger	8

[20] Some countries that were addressed in case studies are not listed here due to concerns about the safety of company personnel. In three cases, the country involved in a case study was not disclosed to the GNI Board on account of such concerns, or because the company was under a legal obligation to refrain from making such disclosure.

Case Examples

This section provides a summary of selected anonymized and non-anonymized cases from the 11 company assessment reports.

Case Study

NOKIA

1) A 4G/LTE Public Safety Network for Government Use in a High-risk Country

This case examined Nokia's human rights due diligence (HRDD) processes surrounding the sale of an LTE-based communications system to a government entity in a high-risk country.

The origins of this case lie in ongoing business development activities, which led to an opportunity to provide a private 4G/LTE public safety network for government use, including by law enforcement and intelligence agencies in a country that Nokia classifies as a high risk for human rights.

The HRDD investigation determined that while the procuring entity and some end users of the public safety network would be domestic intelligence agencies (potentially raising concerns given the human rights risk profile of the country), the project scope would not include any sensitive products or items that would provide any additional or enhanced surveillance capabilities with regard to existing commercial networks in the country. The closed network requested to be supplied would be used exclusively by national security-related agencies and units for their internal communication and would not be connected to any networks open to the public.

Based on these considerations, Nokia's HRDD process issued a "go with conditions" recommendation to move forward on this potential sale. As a condition for engaging in the project, a specific signed certification would be obtained from the procuring agency confirming the nature and purpose of the network.

This case showed the advantages and the limitations of undertaking HRDD at the very beginning of the sales process. It illustrated how the company may provide communication systems and standard networking capabilities to governmental customers for purposes such as public safety, railway communications, and smart city enablement.

2) Advocating Against Direct Access in Finland

This case is about advocating for and promoting the rule of law, transparency, and the principles of legality, necessity, and proportionality in relation to a legislative initiative in Finland to introduce government direct access for surveillance purposes.

Starting in 2015, the Finnish Government launched three legislative initiatives to draft intelligence laws for Finland: one for civilian intelligence, one for military intelligence, and one for an Expert Group to analyze initiatives from the Constitution and human rights perspective. In January 2018, a legislative proposal was published.

Beginning with a statement on the legislative process in 2015, Telia Finland has advocated the company's policy that "governments should not have direct access to a company's networks and systems. The company should retain operational and technical control." The company has advocated this point through meetings and interactions with the Ministry of the Interior and Ministry of Defence. Telia Finland encouraged the lawmakers to be specific and transparent and to be consistent with international laws and standards on freedom of expression and surveillance privacy. Telia Finland has also presented this point in parliamentary hearings of the Committee of Transport and Communications and the Committee of Defence on the spring of 2018 and worked through industry groups such as the Finnish Federation for Communications and Teleinformatics (FiCom) and the Confederation of Finnish Industries (EK).

Telia Finland has also encouraged the Finnish Government to be transparent about the legislative initiative, promoting the rule of law, through formal written positions since 2015.

For transparency, Telia Company in May 2018 reported on the legislative initiative and its position through an article on its company website. Telia Company has also actively engaged with other stakeholders regarding direct access to identify best practices in the field.

telenor group

3) Authority Requests in Myanmar

This case looked at how Telenor Myanmar (TML) handles authority requests with respect to privacy and freedom of expression.

In 2012, prior to entering the Myanmar market, Telenor Group commissioned BSR to conduct sustainability due diligence, in which privacy and freedom of expression challenges related to authority requests were highlighted. The Telenor Group Manual on Authority Requests applied to TML operations from day one.

Although Myanmar's Telecom Law gives the government the right to request confidential information, while protecting basic rights of the citizens of Myanmar, it is not clear on whether the release of confidential information requires a court order. In order to address this issue, Telenor Myanmar built a relationship with the government in Myanmar. The company engaged with authorities responsible for security and police and was able to agree on a set of requirements that would need to be in place in order for the company to respond to a request for confidential information.

As an interim arrangement, pending clearer legislation on this area, Telenor established the following requirements: First, all requests to release confidential customer information shall be sent from the police to the telecom regulator for their consent and must include an explanation of Telenor's obligations under the license together with supporting documentation. Second, independent of the approval from the regulator, Telenor performs its own assessment of each case before deciding to release the requested information or not. A key document as part of this assessment is the First Incident Report which demonstrates that the case has been registered with a Magistrate.

In addition, Telenor Myanmar has not turned on the Lawful Interception (LI) capacity in its network until an appropriate legal framework is in place.

Telenor has successfully established and maintained robust channels of communication with the authorities, enabling it to maintain its policy, which builds on the GNI Principles. These robust channels of communications also allow Telenor to communicate international best practices as the country further develops its legislative framework.

Case Study

4) Blocking Websites in Eastern Europe

The company received a request from a police authority to block access to a number of websites that were allegedly illegal. The company refused and requested a judicial order to block the sites. The company also brought the matter to the attention of the Ministry of Internal Affairs. The government initially launched a case against the company for not complying with the request. The court declared as null the contravention document and sanctions against the company. The court, however, did not say anything about the request to block. The company, therefore, partially objected to the decision and asked the Court of Appeal to comment on the blocking request. As of the end of the assessment period the case had been sent back to the court of first instance and was still pending.

5) Call Data Records Request in Africa

Orange received demands from the national telecommunication regulator of a country in West Africa. The request was to provide access to Orange's roaming management platform, which contains important customer data on roaming calls.

The regulator asked the company to provide all Call Detail Records (CDRs) in an effort to review and control the tax declaration of all telecommunications network operators. The regulator sent the request in a single letter that it addressed to all four operators in the country. Orange's first response was to pursue a common response from the request recipients to lobby the government or otherwise resist the demand more efficiently. The request recipients sent a joint letter to the regulator in response that noted the lack of legal grounds for the demand, and that the demand was in violation of privacy provisions in national and international human rights law.

The government responded by increasing the tax burden for the operators, adding penalties for their refusal to comply with the demand. At this point, Orange alerted civil society organizations about this issue. NGOs denounced the demand on social media and via a letter to the country's Prime Minister. In the end, the Government withdrew the demand, while the regulator asked Orange to pay a large fine for not complying. Orange paid the fine to end the case. A positive outcome from the case was that the government made a public commitment to fundamental freedoms.

This case is an example of sectoral and multistakeholder collaboration to lobby a government to change a policy. The assistance provided by international NGOs and the decision to work with other operators to jointly respond to the government demand clearly contributed to the successful outcome.

Case Study

6) Censorship in Malaysia

This case looked at government requests to censor online content in Malaysia.

Requests to block illegal content are not uncommon, in particular regarding sexual abuse imagery of children and illegal gambling sites. The challenge arises when a request is in the legal grey area or is legal under national law but the sites that are requested to be censored, for example, are credible news sites. These requests raise challenging questions around freedom of expression. This was a particular challenge in Malaysia under former Prime Minister Najib Razak, who was caught up in the "1MDB" scandal.

The company's assessments of the censorship requests were that many of the requests related to news sites that covered a scandal or were critical of government's policies. These requests were escalated with the following assessments undertaken:

- Legal assessment — the assessment was that the authorities had the necessary legal powers to make the request.
- Human rights assessment — identifying the challenge to free speech for some of the blocked sites.
- Security assessment — no significant risk.

The result of the assessments was that the government had the legal authority to make this request. To minimize the impact, the company took actions to be transparent about which sites were censored. This case demonstrates that in cases where it is legally obliged to comply with authority requests, a company can still work to minimize negative impacts by promoting transparency.

Case Study

7) Challenging a Gag Order in the United States

This case explored a situation in which Facebook challenged gag orders prohibiting the company from disclosing the existence of three search warrants it received seeking information regarding accounts held by people who were suspected of involvement in alleged criminal activity arising from protests associated with the presidential inauguration on January 20, 2017.

In line with the GNI Principles and Implementation Guidelines, and as disclosed in Facebook's Information for Law Enforcement Authorities, Facebook provides notice to people who use its service of requests for their information prior to disclosure unless Facebook is prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies, or when notice would be counterproductive.

Facebook challenged the gag orders as violating its right to free speech under the First Amendment to the U.S. Constitution. Facebook challenged the gag order before the lower court, and, when that court denied Facebook's request, Facebook appealed the case at the District of Columbia Court of Appeals. In response to Facebook's legal challenge to its gag orders, the government withdrew them and agreed to let the company notify the affected account holders. As part of this process, Facebook also solicited amicus curiae briefs from interested external stakeholders, including GNI company and non-company members.

This case illustrates several issues relevant to Facebook's implementation of the GNI Principles, including the company's efforts to challenge demands it believes to be overly broad in domestic courts and its approach to engaging with external stakeholders, including GNI members.

Case Study

8) Content Removal Request from Russia

In 2017, the Russian government authority "Roskomnadzor," the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media, issued three requests to a company to remove content related to the same piece of content posted by a single user. All three requests explained that Roskomnadzor had determined that the content at issue contained what they alleged was child sexual abuse content. Each time, Roskomnadzor requested the removal of the specific image within 24 hours, warning that access to the company's service would be limited if action was not taken.

Taking account of the potential that its services might be blocked, the company assessed each request against its relevant policies. Since the content at issue was an artistic image and did not depict child sexual abuse material or violate the company's policies, no action was taken. The company sent a standard response to the requesting agency stating that it had investigated the case and taken any appropriate action consistent with its policies and received no further requests after it sent its reply.

This case demonstrates that even when faced with pressure to its operations, a company can take steps to follow established policies and to attempt to minimize impacts to free expression for its users.

Case Study

9) Content Request from Europol's EU Internet Referral Unit ("EU IRU")

In May 2018, a company received a request from the European Internet Referral Unit ("Europol") stating that it had detected specific pieces of terrorist content on the company's platform that could potentially violate the company's terms and conditions. The request included a list of specific universal resource locators (URLs). The request was escalated given the nature of the content at issue and reviewed by appropriate personnel within the company. It was determined that the content unambiguously violated the company's publicly available policies because it depicted content that was supporting or celebrating a terrorist organization, Islamic State of Iraq and Syria (ISIS). The company took action on the content consistent with its policies. The company then informed Europol that appropriate action was taken consistent with the company's policies. This case demonstrates how escalation procedures work in practice inside a company.

10) Data Retention in Sweden

On December 21, 2016, the European Court of Justice (ECJ) ruled that the EU Data Retention Directive did not meet human rights requirements and that requiring general data retention is not proportionate. Telia Company informed the Swedish National Regulatory Authority that it had therefore stopped retaining data according to national Swedish legislation based on the Directive. In response, a government minister, as well as prosecutors and representatives of the police, publicly demanded operators to retain data on a voluntary basis. A follow-up meeting was held with the Minister of Internal Affairs and another meeting with relevant authorities. In these meetings, Telia Company voiced its position not to retain data in relation to Sweden's specific data retention provisions.

On December 30, 2016, Telia Sweden published a statement that said the company could not continue to retain data according to the provisions in the Swedish law implementing the EU Data Retention Directive. The statement also noted that Telia Sweden does, however, retain data according to general but limited provisions in the telecommunications legislation, so that such data is available to law enforcement according to due process, rule of law, necessity, and proportionality.

As of the end of the assessment period, the Swedish legislature was preparing changes in national law following the ECJ ruling. On January 30, 2019, Telia Sweden provided comments on the new legislative proposal, arguing that there should be no broadening of data retention; the need for transparency; the need for proportionality and necessity; a distinction between data retention for law enforcement and data retention for commercial use; that costs for law enforcement including data retention should be transparent; and, finally, the clear risk that the proposed new law will, again, be overruled. Telia consequently asked for the proposal to be reworked. This legislative proposal was logged in Telia Company's list of unconventional requests with potentially serious impacts on the surveillance privacy of the company's users.

11) Digital Fingerprint Bill in Paraguay

This case examined Millicom's efforts as part of a multistakeholder coalition to defeat the enactment of a law that would have required telecommunications network operators in Paraguay to collect fingerprints from new and existing customers as a condition of providing them with mobile phone service.

In November 2015, a bill was introduced in the lower house of the Paraguayan Congress to "regulate the activation of mobile telephony services." The bill would require mobile network operators to collect a full set of fingerprints from their new and existing customers. Should an operator fail for any reason to collect fingerprints from an existing customer within a year of the bill's enactment, the operator would be required to cut off service to that customer. Other provisions of the bill would place personal liability on company officials for any failure to comply with the law.

Millicom's in-country team met with representatives to highlight the company's significant concerns with the proposed legislation. Millicom also worked through the local Chamber of Mobile Operators to coordinate an industry-wide effort to oppose the bill. Representatives were apparently unmoved by these efforts and continued to champion the bill in Congress.

In August 2016, the Bill advanced rapidly through both chambers of Congress and transmitted to the President for his signature. A multi-pronged strategy was deployed to try and secure a presidential veto on this legislation, including the following actions:

- Tigo (Millicom) and the other member-companies in the Chamber of Mobile Operators mounted a publicity campaign to alert the public to the dangers of this ill-considered legislation.
- Millicom's in-country Corporate Affairs team began an effort to brief and explain concerns regarding the proposed Bill to different government stakeholders, including Office of the President and members of both Houses of Congress.

- Millicom's global external affairs team leveraged their relationships with key members of the international human rights community to focus the spotlight of global attention on this proposed Paraguayan measure.
- Members of Millicom's global corporate responsibility team reached out to representatives of TEDIC, Paraguay's leading digital rights NGO, to explore how they could work together to convince the President to veto the bill.

The efforts of Millicom and its numerous partners to oppose the "fingerprint law" met with success on September 25, 2017, when the President vetoed the Bill. As Congress did not seek a veto override within the six-month timeframe provided by the Constitution, there is no possibility of the Bill now becoming law unless it is reintroduced.

This case demonstrated Millicom's ongoing efforts in countries such as Paraguay to engage and dissuade legislators from advancing laws that might sound good on paper yet are flawed in practice. The case showed how Millicom leveraged the different relationships and skillsets of its in-country and corporate-level personnel in responding to the challenge posed by the Paraguayan legislation.

Case Study

12) Emergency Request for User Data from a Western European Country

This case examined a company's handling of an emergency government request for information of an email user in a western European country. This was part of an effort to locate and arrest an individual suspected of planning an imminent terrorist attack.

In 2018, the company received an emergency request from a law enforcement agency that has jurisdiction over major crimes in a city in western Europe. The request sought information pertaining to a specific account in order to locate and arrest an individual believed to be planning an imminent terrorist attack in that country. The request was in writing on the law enforcement agency's official letterhead and signed by an appropriate official. It was transmitted in its original local language accompanied by an English translation. The request sought basic subscriber information for a particular account as well as additional contact information and IP logs. The request was reviewed pursuant to the company's procedures. Finding that the request pertained to a bona fide emergency involving the potential of significant loss of life, the company responded by disclosing the basic subscriber information it possessed regarding the specified account to the law enforcement agency.

This case illustrates a company's policies and procedures for responding to emergency requests from governments. It shows the functioning of a company policy of responding to such requests with the least amount of data required to respond to the emergency. There is always a concern that governments may misuse these emergency requests to obtain data from companies in situations that do not meet the stringent criteria for such emergencies. Providing the minimal amount of responsive data that is reasonably connected to the government's objective provides an appropriate safeguard against the possibility of misuse.

Case Study

Telefónica

13) Grievance Mechanism at Global and Local Level (example: Colombia)

This case illustrated how Telefónica has set up mechanisms at the global and local level to respond to human rights grievances reported by stakeholders, including those regarding privacy and freedom of expression.

Telefónica created its Responsible Business Channel in 2016, an external grievance and remedy mechanism in line with the UN Guiding Principles on Business and Human Rights. The Responsible Business Channel was complemented with a grievance and remedy mechanism at the country level to better capture local realities — implemented first as a pilot in Colombia. The objective of complementing the global with a local mechanism was to identify, manage, and remedy any human rights queries and complaints reported through local company channels.

The global Responsible Business Channel was designed as a one-stop-shop for stakeholders to consult or make complaints on human rights issues. Special attention was paid to design the Channel in accordance with requirements laid down in the UN Guiding Principles on Business and Human Rights. In 2016, the Responsible Business Channel was officially launched. Ever since, Telefónica has publicly reported the number and types of complaints it receives in its Consolidated Management Reports. In 2019, a Group Regulation about the Management of Responsible Business Channel was updated to reinforce a uniform handling of complaints across all markets.

A local level grievance and remedy mechanism was also set up by Telefónica Colombia to facilitate the filing of complaints by local stakeholders about respect to human rights, the environment, and reputation. An initial stocktaking was carried out to identify all the touch- points/communication channels the company had with customers in order to find out how human rights-related complaints could potentially be made and what procedures were followed in each case. On this basis, in 2017, a streamlined procedure was designed for receiving, processing, and resolving the complaints coming from these various channels with a view to giving a rapid and diligent response to any complaint made.

Case Study

In sum:

- The Customer Service Area, which receives all types of queries and complaints, sends the complete base of all non-service-related queries and complaints to the Sustainability Department, which in turn identifies relevant grievances and classifies them accordingly in a database.
- In case the corresponding department resolves the complaint, the solution is communicated to the interested party and concluded with a negotiated resolution and remedy agreement, thus closing the case.
- In case direct negotiation with the interested party fails, the parties may use a mechanism provided for in Colombian law: a prejudicial conciliation, before considering recourse to the judiciary.

While 182 complaints were received on human rights issues in 2017 (of which 29 had high priority), 215 complaints were received on human rights issues in 2018 (of which 30 had high priority). However, in neither year was there a complaint in matters relating to privacy or freedom of expression.

Case Study

Telefónica

14) Human Rights by Design

This case showed how Telefónica incorporated the evaluation of any potential human rights impact, including freedom of expression and privacy, at the outset of designing and/or marketing products and services.

In its 2017/2018 human rights impact assessment the company noted a need to consider human rights aspects when designing or developing products and services. In response, the company reviewed the different processes for the design and marketing of products and services to identify how and at what stages in these processes human rights considerations could be incorporated, as well as the types of rights that might be affected.

Following the completion of a stocktaking exercise, the company developed a "self-assessment process" that included questions related to the rights to privacy and freedom of expression, as well as the ethical use of artificial intelligence and the impact of the product or service on the environment. Several pilots were conducted with business areas of the company and finally a self-assessment tool was made available to all employees of the company via the intranet but aimed specifically at product managers.

After these pilots, the final questionnaire includes three types of impacts on:

1. The customer: With respect to simplicity, transparency and integrity of products/services offered.
2. The environment: Aspects of waste, eco-design, recycling, energy saving, and positive environmental impacts are considered.
3. Society: Assessing aspects of human rights, diversity, impact on vulnerable groups, privacy, freedom of expression and other issues that may have a negative impact when the product and/or service incorporates artificial intelligence.

Case Study

Google

15) Implementing Germany's Network Enforcement Act

This case concerns Google's implementation of Germany's Network Enforcement Act (Netzwerkdurchsetzungsgesetz or NetzDG), which requires online companies to remove certain content within 24 hours of notification, and other content within 7 days.

NetzDG went into effect on January 1, 2018. It is arguably the most ambitious attempt by a Western state to mandate specific actions by social media platforms to remove online speech deemed illegal under domestic law. While NetzDG has encouraged accountability and transparency from large social media platforms, it also raises critical questions about freedom of expression and the potential chilling effects of the legislation.

When the law was proposed, Google responded with a multi-pronged approach. Google's internal working group included personnel from the policy, removals, law enforcement and information security, government affairs and public policy, and legal counsel teams (including outside counsel). Google publicly advocated extensively against the legislation, citing risk to freedom of expression from overblocking, due to the potential penalties for failure to meet timelines. The company engaged with key external stakeholders to make clear the impact on freedom of expression the proposed law could have. Together, human rights stakeholders succeeded in turning back a requirement of proactive filtering, as well as some other requirements.

After the law was enacted and went into effect, Google built an implementation program that was designed to address the risk of overblocking by clarifying content policy and providing additional internal interpretive guidelines to the removals teams. Google hired numerous reviewers and provided reviews around the clock, to support a meaningful assessment of whether the content reported for removal was in fact illegal.

Content removal complaints were examined the way Google analyzes removal requests from governments. Google considers whether the content violates Google's community guidelines, whether it clearly violates a local law, and whether the content is related to a matter of public

interest, such as political speech. If the content is marked for takedown, Google removes the content only in the local jurisdiction, unless it clearly violates its own community guidelines.

Google then built a mechanism to encourage reports that were more on point with the actual conduct and connected to possible violations of the law or guidelines. Google also devoted substantial training and resources so that individual removal requests could be reviewed appropriately to address freedom of expression concerns. Creating a clearly defined intake process, coupled with a specifically trained team to handle complaints, allowed Google to more efficiently identify complaints that did not involve speech that was illegal or against its guidelines. All removals are reflected in Google's transparency reports.

Case Study

verizon media

16) Implementing the GNI Principles within Verizon Media

This case explores how the GNI Principles were adopted within Verizon Media after Yahoo's acquisition.

In spring 2008, Yahoo launched the first dedicated team within the industry focused on examining business impact on human rights. The Business & Human Rights Program ("BHRP") was created to lead the company's efforts to make responsible business decisions in the area of human rights, including free expression and privacy. Nearly a decade later in 2017, after Yahoo's acquisition, Yahoo was joined with AOL to form Verizon Media (formerly Oath). Yahoo's BHRP was immediately tasked with building out its Program across Verizon Media's house of media and technology brands. The strategic approach that Yahoo established to managing human rights risk was adopted by Verizon Media and the BHRP was empowered to lead the company's efforts to protect privacy and freedom of expression. The build-out of the BHRP across all of Verizon Media's brands was a key priority for senior leaders within the company, with whom the Global Head of Business & Human Rights consulted on how to ensure a successful transition.

Certain early priorities were identified, including:

1. Governance and Oversight: Establishment of governance and oversight for human rights issues at Verizon Media;
2. GNI Commitments: The transfer of Yahoo's GNI membership to Oath (now Verizon Media) and the integration of the GNI Principles across Verizon Media, including within AOL, which had not previously been a GNI member;
3. Education and Awareness: Internal education about the BHRP and its issues and also about the GNI; and

4. Internal Decision-Making: Attention to integrating the BHRP and its practice of conducting human rights due diligence and impact assessments into decision making processes within Verizon Media, including related to the integration and alignment of policies, processes, and systems.
5. Transparency: Within months of its acquisition, Verizon Media produced a new Transparency Reporting Hub containing reports on government requests for user data and content removal, as well as Tumblr's Copyright & Trademark report. The BHRP was enlisted to advise on ways to standardize the reports of Verizon Media's brands AOL, Yahoo, and Tumblr and to ensure the new, combined disclosures tracked to the highest level of transparency across the different reports that existed previously. In addition, the BHRP published its new webpage.

After the assessment period ended, Verizon announced that the BHRP team would be further expanded to support the entire Verizon business, while also continuing to support the Verizon Media business. The decision taken by Verizon to establish the BHRP across the whole parent company demonstrates the continued and growing strategic priority given to its work.

Case Study

17) Network Shutdowns in Pakistan

Some network operators receive requests to shut down parts of or the entire mobile network. This case illustrates how this is handled in Pakistan, where it happens fairly regularly.

In Pakistan, shutdowns have occurred fairly regularly for many years. Telenor Pakistan (TP) has worked over the years to engage with the relevant authorities to put in place processes for receiving such requests in line with local law and Telenor's requirements (to not impose significant risk of non-proportionate limitations to human rights). Topics like the scope and duration of a request have been discussed, with a view to get requests to cover smaller areas and last for shorter periods of time. There are legitimate security concerns and it has been important to acknowledge this in the company's dialogue with the authorities, whilst also seeking to prevent or mitigate any adverse human rights impacts. Over the years, TP has experienced that the requests have become more targeted and surgical, covering smaller areas, shorter time periods, etc. This is believed to be in part due to the ongoing dialogue that TP has with the authorities. However, the challenge of shutdowns continues to exist.

The Institute for Human Rights and Business (IHRB) Digital Dangers Study outlines the efforts made by Telenor Pakistan to address the challenges and sets out the socio-economic impacts of shutdowns.[21] This study was also included as part of the petition to the 27 Islamabad High Court, which in February 2018 ruled that shutting down networks is illegal. The order has since been appealed against in the Supreme Court, which has suspended the order until final disposal of the Appeal. It is not yet known when the case will be heard by the Supreme Court. With regards to lessons learned, Telenor sees a need for continued engagement with Pakistani authorities over time. This challenge will not go away any time soon. Also, it is important that dialogue is constructive and collaborative, and not confrontational, as this may hinder progress.

In the case of Pakistan, Telenor has demonstrated that the protection of employee safety is paramount, necessitating compliance with shutdown requests. Nevertheless, Telenor has successfully engaged with the relevant authorities to ensure a narrower interpretation of such requests, reducing the potential impact.

[21] Although written prior to the reporting period for this assessment, the study provides important background for understanding how TP handles shutdown requests.

Case Study

18) Prison "Signal Blocking" Laws in Latin America

Organized crime is a serious concern in several Latin American countries. In some cases, leaders of gangs have continued operating criminal empires from within jail cells. In recent years, governments have passed laws mandating mobile network operators to take all necessary steps to prevent their services from being accessed within prisons, imposing severe penalties for operators that fail to comply. In such cases, companies strive to ensure that the application of the law would minimize any adverse effect on the wider population.

Following initial measures to comply with these laws, the company reported that it took the following measures to minimize their impact:

- Engagement with different ministries to explain the physical impossibility of strictly complying with the laws without some adverse effect on the nearby population; and the measures that could be taken to effectuate the laws' aims while minimizing the impact on the overall population.
- Work with regulators to fine-tune its approach to implementing the signal blocking mandate. These measures reduced the areas affected to a radius of between 200 and 500 meters around the prison. The company bore the full cost of implementing these measures, including construction of new base stations.
- Collaboration with civil society organizations and affected community members to identify ways to mitigate the disruptions. These measures included installing lower-powered base stations to serve certain communities and adjusting antennas to transmit in certain directions.
- Partnerships with industry associations to engage legislators and regulators, including the development of a policy statement on the issue.

Given the significant on-the-ground presence required to provide services in a given area, companies face pressures to comply with local law in view of risks to safety of equipment and personnel. The company's initial measures to comply with the law were a reasonable short-term means of promoting its long-term objective of providing telecommunications services

in these countries in a rights-respecting manner. The materials reviewed and the interviews conducted by the assessor suggest the company did all it could to minimize the short-term disruptions in service caused by the laws. More importantly, the company almost immediately began to take measures to mitigate the unintended disruptive impact of its initial actions to comply with the law. These measures, which have required significant expenditures in equipment and personnel, speak to the depth of the company's commitment to maximize access to its services and minimize adverse impacts on its customers.

Case Study

19) Request to Remove LBGT Applications in Asia

This case concerns an Asian government's request to a company to remove 65 lesbian, gay, bisexual, and transgender (LBGT)-related applications, including dating services, from its application platform.

The company's review identified that the request to remove the LGBT apps came with a threat of police actions and potential blocks on the company from operating in the country. The company sought a way to navigate this without putting local employees at risk and avoiding a situation where its app platform would be blocked.

The company broke its response into categories of review before making an individual decision on each app that the government had complained about. They first considered whether any of the apps individually violated any developer content policies or terms of use. Second, the company examined whether content in any of the apps directly violated any local laws that the government was concerned about, such as obscenity laws. Third, the company considered whether any identified issues were correctable by the app developer. Fourth, the company considered what impact the removal could have on human rights.

Since these apps were focused on connecting the LGBT community, the company identified freedom of expression and association as key issues at stake. Several apps contained content that was in violation of the company's own policies, or the non-discriminatory application of the local obscenity laws. The company asked for the removal of such content. Where the apps as a whole were clearly in violation of local obscenity laws and could not be corrected, they were removed from the app platform. The company sought clarification from the government on the request for the remainder of the apps.

In responding to what could have been a mass blockage of apps that allowed members of the LGBT community to connect and associate, the company took a balanced, most restrictive response approach where decisions favored keeping the apps available. In this case, despite company shut down and raid pressures from the government, the company identified a balanced process that removed those apps that were in fact violating the company's own policies, while leaving up the rest, pending further information from the government that would warrant removal.

Case Study

20) Responding to Blocking Orders in Eastern Europe

In 2017, Orange's local CEO received a request from the police to block access to a defined list of websites that were allegedly used to sell drugs.

This request was received by the local CEO in late 2017, who notified the CSR manager for Europe and local and Group legal departments. Their examination concluded that local law did not expressly state the obligation of an operator to block access to web resources based on inquiries from law enforcement agencies. This case involved several local laws which provided some legal grounds for the blocking request but was open to interpretation by the company.

Orange based its evaluation of the request on the GNI Principle that "restrictions should be consistent with international human rights laws or standards, the rule of law, and be necessary and proportionate for the relevant purpose." In this case, the company found the purpose of fighting drug sales to be relevant and proportionate. Orange partly complied with the request. Visitors to the blocked sites informed that they were categorized as "harmful" with access restricted. This provides notice and transparency to users.

Case Study

NOKIA

21) Standard Location Tracking in an Extreme Risk Country

This case evaluated Nokia's handling of a potential sale of 3rd Generation Partnership Project (3GPP) standards-compliant equipment to geolocate cellphone users to a nongovernmental private entity in an extreme risk country.

This case arose out of a request for proposals (RFP) issued by a nongovernmental private entity operating in a country Nokia considers to be an extreme risk for human rights. Under 3GPP standards, such a solution may be used to very precisely locate a user in case of emergencies, either when the user calls the local emergency access number, or for purposes of sending out an emergency alert to all mobile subscribers in a certain geography.

The 3GPP compliant use case is related to emergency services, such as disaster alerts, or targeted advertising, with no real-time user information storage. The authority request was to integrate this solution with a surveillance system provided by a third party, and to provide a historical database on user information for authority use. The investigation focused on the request on the nonstandard development & implementation of the historical database with access to a LI authority application. The creation of a historical database with an integrated interface to authorities would have enabled unlimited access to subscriber data with an undefined scope of governmental agencies in the target country, thus negating the principles of necessity, proportionality, or legality on authority use of end-user data. Furthermore, no standard LI solutions would have been used, only standard database creation with normal systems integration and interface creation — making this case an excellent example of the "dual use" dilemma, highlighting the importance to focus on the intended use of technology, instead of monitoring single product items.

In view of these findings, and especially given the scope of the human rights risks associated with the indefinite storage of cell phone geolocation information, Nokia's internal HRDD process unilaterally concluded a "NO GO" recommendation with regard to this potential transaction. Nokia notified the potential customer for this transaction that Nokia concluded it could not provide it with this particular set of solutions at this time.

Case Study

This case illustrated how Nokia's HRDD processes focused on examining the risks to human rights by the particular use to which standards-compliant communications technologies with important public safety functions are to be used, rather than focusing on the nature of the technology itself. It also shows how Nokia assessed whether the legal regime in a given country was consistent with international human rights standards and norms in determining the level of human rights risk that a particular proposed transaction poses.

NOKIA

22) Whether to Provide a Standard Platform Switch in an Extreme Risk Country

This case showed how Nokia's human rights due diligence process evaluated a request from a non-governmental private entity in a country Nokia considers to be an extreme risk for human rights. The case illustrated the company's approach to HRDD in the "dual use" context — evaluating the human rights risks from products that are not specifically designed for communications interception purposes, but whose capacities are nonetheless susceptible to being misused by governments to engage in unlawful surveillance.

The case arose out of a request from a non-governmental private entity to purchase a standard local access network (LAN) platform switch. This is a high-speed, high-capacity piece of networking equipment of the sort that Nokia routinely sells to its telecommunications customers around the world. Due diligence revealed that the switch would function as a data aggregator to push all aggregated Internet traffic data onto the local lawful interception server.

Given the request for unlimited and undefined authority to access subscriber data, it would not have been possible at all to ensure the principles of necessity, proportionality or legality, nor ensure any transparency on the authority use of intercepted data. Furthermore, no standard LI solutions would have been used, but only standard broadband products, again highlighting the importance to focus on the intended use of technology, instead of monitoring single product items. Through Nokia's HRDD process, Nokia unilaterally concluded this was a "NO GO" and the company declined to proceed.

This case illustrated the functioning of Nokia's internal HRDD processes, particularly regarding the emphasis the company places on determining the uses to which a particular product will be put in evaluating the level of human rights risk posed by the potential sale.

Company Determinations

After a detailed review of the confidential assessment reports and discussions with the companies and assessors, the multistakeholder GNI Board made its determination for each company. A finding of compliance indicates that the GNI Board determined that during the assessment period, the company made good-faith efforts to implement the GNI Principles with improvement over time.

UNDERSTANDING THE GNI BOARD REVIEW AND DETERMINATION

In preparation for the review of 11 company assessments, more than twice as many as in any previous assessment cycle, the GNI Board aimed to ensure that the review process was both as manageable and as meaningful as possible. Highlights include:

Multiple Assessment Review Meetings: Rather than attempting to review all of the company assessments during one meeting, the GNI Board dedicated a full day at each of three board meetings in March, June, and October 2019 for assessment review, as well as a portion of a day in November.

Presentation and Q&A: For each review, assessor and company presentations to the GNI Board were followed by Q&A for a minimum of one hour. This was followed by separate additional Q&A and discussion between the GNI Board and the company.

Study Groups and Questions: The non-company constituencies of the GNI Board formed study groups to focus their review of each company assessment. Study groups met in advance of the review meeting and prepared questions that were shared with the company, assessor, and the rest of the GNI Board shortly before each assessment review meeting. Many of these questions were addressed during the question and answer period at the board meeting.

Voting Process: The board's determination is subject to a super-majority vote, which is defined as two-thirds of the full board and at least 50 percent of each constituent group. As few as two negative votes in the investor or academic constituency, or three negative votes of the NGO constituency, results in a finding of non-compliance. This did not occur during this assessment cycle. The company undergoing assessment is recused from the vote.

"The non-company members of the GNI play a critical role in ensuring the integrity of the regular company assessment process. Working with our global network of member organizations, the non-company board members identify specific cases for review that highlight key challenges and illuminate company progress in implementing GNI commitments. Prior to our formal board session, the non-company board members meet in study sessions to review company assessment reports, which help to focus and frame our engagement with companies and their assessors during the formal board review session. During the formal board session, the non-company board members surface recommendations for improvement, as well as priorities for the GNI Learning and Policy committees, which form an important part of GNI's agendas moving forward."

MEG ROGGENSACK, Georgetown University Law Center

The following section provides the determination for each company as well as a summary of information that can be made public from the company's assessment report. **For each company, the description of its operations, products, and services under "The Company" is provided by the company.** As described in the Assessment Toolkit, each assessed company decided whether they or the assessor would draft the initial response to the questions, with certain exceptions.[22] When companies drafted the initial responses, the role of the assessor was to review and verify these answers, for example by asking additional questions and requesting additional verifications.

[22] For the Process Review, Section 1 (Context of Assessment) and Section 6 (Follow Up and Improvement) must be drafted by the assessor. For the case studies, Section 4 (Assessor Comments) should be drafted by the assessor.

METHODOLOGY FRAMEWORK

- GNI Principles
- Implementation Guidelines
- Assessment Toolkit
- Process Review Questions
- Case Study Template
- Relevant Excerpts from Governance Charter and Accountability, Policy and Learning Framework
- Mapping the GNI Principles to Implementation Guidelines
- 2015/2016 Public Assessment Report
- Assessment Q&A

Facebook

The GNI Board conducted its second assessment review of Facebook and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Facebook, incorporated in 2004, is a global technology company with a mission to give people the power to build community and bring the world closer together. Building on the social network platform of the same name, Facebook has acquired other companies in the past and offers now also web and mobile-based messaging services and a dedicated image/video-sharing platform. Total revenues amounted to $55.838 billion for the financial year ending in December 2018 ("FY 2018").

As described in Facebook's annual report, Facebook currently offers services to users through five brands with relevance to the scope of this assessment: Facebook, the company's namesake social media platform; Messenger, a messaging platform fully integrated with the Facebook graph; WhatsApp, an end-to-end encrypted messaging service; Instagram, a photo and video-centric social media platform; and Oculus, a virtual reality company.

Facebook's products are generally available worldwide unless a government actively blocks the service.

Facebook

Governance

On a day-to-day basis, implementation of the GNI Principles at Facebook is primarily the responsibility of a dedicated Human Rights team. Since Facebook's last GNI assessment cycle in 2015/2016, Facebook's corporate structure has fully integrated Instagram and WhatsApp, with the same structure exercising primary oversight of the implementation of the GNI Principles across the company's products.

Due Diligence and Risk Management

All new or substantial changes to product features or proposed uses of user data must go through a systematic review for potential privacy impacts. Similarly, the Content Policy team evaluates changes to policies that may implicate freedom of expression. The Human Rights team is involved in both of these processes, which serve as formal mechanisms for conducting human rights due diligence in line with the GNI Principles and Implementation Guidelines and the UN Guiding Principles on Business and Human Rights.

Where this initial due diligence raises significant new human rights concerns, Facebook's Human Rights team may conduct a more in-depth human rights impact assessment (HRIA). The company noted that this most often occurs in the case of creating a physical presence in a new country, launching a major new product or service, substantially modifying policies or practices related to freedom of expression or privacy, or when it becomes aware of information suggesting that Facebook's platform is posing novel human rights impacts in a specific country.

Facebook conducted a number of HRIAs during the assessment period, including an independent HRIA on its impacts in Myanmar, which it published in full.

Freedom of Expression and Privacy in Practice

Facebook has detailed policies and procedures — informed by the GNI Principles — for responding to government requests related to both disclosure of user data and content restrictions.

The company publishes key elements of their process for responding to government requests for user data in the Information for Law Enforcement page on its website. Instagram and WhatsApp offer similar information with differences arising from the characteristics of each product and the types of information they collect, use, and store.

Transparency and Engagement

Facebook informs its community of stakeholders of its approach to human rights issues, via a dedicated Stakeholder Engagement team, regular updates on the Facebook Newsroom covering relevant freedom of expression and privacy issues, publicly available policy documents such as the Community Standards, and a biannual Transparency Report, detailing its process for responding to government requests to remove or restrict content.

Additional information on applicable policies, procedures, and legal obligations related to freedom of expression and privacy is disclosed in the Community Standards and Instagram Community Guidelines; in the Information for Law Enforcement Authorities for Facebook, Instagram, and WhatsApp; and in the information accompanying Facebook's biannual Transparency Report.

As specified in the company's Law Enforcement Guidelines, Facebook's policy is to "notify people who use Facebook's service of requests for their information prior to disclosure, unless Facebook is prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive." Facebook will also provide delayed notice upon expiration of a specific non-disclosure period in a court order and where they have a good-faith belief that exceptional circumstances no longer exist, and the company is not otherwise prohibited by law from doing so.

As stated in the company's Transparency Report, Facebook also provides notice to users whose content is restricted on the basis of local law in response to government requests, as well as to users who attempt to view such content, except where such notice is legally prohibited or where technical constraints prevent it from doing so.

For general privacy-related grievances, privacy policies for Facebook, Instagram, and WhatsApp provide information on how to directly contact Facebook's Global Privacy Team, and, if applicable in a user's jurisdiction, Facebook's designated Data Protection Officer and the relevant Data Protection Authority.

For decisions made to remove content under Facebook's Community Standards, including actions that are taken on the basis of reports made by governments, Facebook offers an in-product appeals process.[23]

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. Since the last assessment, the assessor reported that Facebook has strengthened its systematic review of both privacy and freedom of expression.

During the previous assessment, the assessor made recommendations in nine areas for Facebook to consider. The assessor noted that actions taken by the company have fully addressed three of these areas. In the case of five recommendations, Facebook has taken actions to address the recommendation and the assessor has recommended

[23] At the time of writing Facebook was in the process of launching an Oversight Board to provide for further independent review and serve as a remedy mechanism for user grievances related to content removal.

Facebook

additional follow up in specific areas. In one recommendation, Facebook has made a number of changes based on the recommendation but has chosen not to implement one aspect due to a difference of views regarding the impact that adopting the recommendation could have on user rights.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement. One example of an assessor recommendation to Facebook is to take additional steps to specifically address the way safeguards for privacy and freedom of speech are implemented with regards to third party relationships.

Google

The GNI Board conducted its third assessment of Google and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Google's mission is to organize the world's information and make it universally accessible and useful. Google's goal to "develop services that significantly improve the lives of as many people as possible," is guided by internationally recognized human rights standards.

Google's core products and platforms such as Android, Chrome, Gmail, Google Drive, Google Maps, Google Play, Search, and YouTube each have over one billion monthly active users. In addition to consumer software products and platforms, Google has an enterprise-oriented cloud business, and a hardware devices business. As of September 30, 2019, Google had 114,096 employees. A global company, Google's headquarters is located in Mountain View, California, and it has 70 offices around the world, including in Africa, Asia, Europe, North America, and South America.

Google is a subsidiary of Alphabet Inc.

Governance

Senior management oversees the implementation of the GNI Principles at Google and provides quarterly updates to the Board of Directors on relevant issues. The company has implemented an intricate network of personnel designed around product, jurisdiction, and functional areas who are responsible for the day-to-day operations of protecting user rights of freedom of expression and privacy. This network is best described as a matrix that has direct oversight by senior personnel and is supported by a global human rights policy lead. The matrix includes: dedicated teams, to review and process government requests for user data and content removal or restrictions; counsel, who are assigned to specific products and regions and provide support on legal and policy issues; and policy experts, assigned to products, countries, and functional areas, who identify and address implications and risks to freedom of expression and privacy of Google operations.

Due Diligence and Risk Management

Google has product-specific counsel embedded with product teams who are part of the development of any new products or features. These product counsel serve as the initial eyes and ears for raising potential risks to freedom of expression or privacy. Product and regional counsel, in coordination with subject-matter and regional experts among the policy staff, assess jurisdiction-based risks to freedom of expression and privacy. This includes review with local outside counsel who are experts in the applicable law in a jurisdiction, including the strength of the domestic legal system with regard to addressing user privacy and freedom of expression.

Google takes a multi-pronged approach to mitigate risks that are identified during any due diligence on an ongoing basis, for example balancing jurisdiction-specific restrictions and global availability. Google uses multiple teams from policy, law enforcement, content removal, government affairs, public policy, outside counsel, and centers of excellence when making mitigation decisions on matters impacting privacy and freedom of expression.

Freedom of Expression and Privacy in Practice

At Google, a dedicated team designs, implements, oversees, and revises the policies for responding to government requests for user information. Other dedicated teams have the same role for removals from YouTube, and products other than YouTube.

Governments are required to follow established legal processes in their home jurisdictions. Google assesses the legal validity of the request, both in terms of the authority of the issuing entity, and the application of the relevant local law. It is Google's policy to object or return the request if these requirements are not met.

Google evaluates requests against human rights standards, and takes several measures to narrow requests, consistent with the GNI Principles. First, it carefully examines the domestic law cited to assess its specific requirements and application to the particular data access or removal requested. If the law is ambiguous, Google may interpret it in a narrow

manner to avoid or restrict the government request. Next, its practice is to apply domestic law only to content and data within the scope of the issuing jurisdiction.

At the granular level, when provided unclear government removal requests, where possible, Google reaches out to the relevant government entity to seek clarification on how the content is violating local laws, where the content is exactly located (i.e., specific URLs), and exactly which portion of the content in question is alleged to be infringing the relevant regulations/restrictions. Similarly, for data access requests, Google may reach out to a government submitter to see if an overbroad or vague request can be cured by narrowing and focusing the request to enable compliance under Google standards.

The company assesses the risks of individual jurisdictions in determining where data is physically collected, stored, and retained. Related to this, Google considers similar risks in determining the jurisdictional footprint of particular products. The company may vary the nature of data collected or processed in particular jurisdictions based on these risks. The company also uses encryption, and limits on internal access, to mitigate risks to data that is collected and stored.

Transparency and Engagement

The Google Transparency Report outlines the company's approach to government removal and user data requests and discloses the company's response to requests. The report covers numerous areas where government conduct may impact freedom of expression or privacy that contain significant amounts of information deserving of a careful review by the public, policy makers, and civil society. In addition, company executives and staff issue public blog posts and testify on freedom of expression and privacy issues globally. Individual products provide their own statements of values (e.g., YouTube four freedoms; Blogger content policy). The company has a page dedicated to its human rights commitment as part of its "About" page. Finally, company representatives also meet regularly with regulators and NGOs on these issues, and conduct ESG investor calls.

Google's Privacy Policy clearly delineates what information is collected and how it is used, shared, or disclosed. The Privacy Policy covers all products and where specific changes exist, the policies make note of that for the user. In addition, the Data Transparency project provides detailed information on data collected.

Google provides information on laws and policies that may require the company to restrict or disclose content or communications through multiple channels such as the Google Transparency Report, Community Guidelines, Privacy Policy, Terms of Service and legal removals page.

Google

Google makes its Privacy Policy, Community Guidelines, and Data Transparency pages publicly available. In addition, the Google Transparency Report provides further information on its policies and procedures.

Google's practice is to notify users when content is removed due to a government request by emailing the user and by placing a notice where the content used to be, informing any visitors of the same. Google will send these removal notices to Lumen, a content removal transparency project of the Berkman Klein Center at Harvard University.

Where data is disclosed to a government agency pursuant to legal process, Google will notify the user whose data was disclosed, unless it is specifically and clearly restricted by law from doing so. For requests from governments outside the U.S., this is generally limited to civil/administrative requests, due to secrecy laws.

Users are provided the ability to appeal removal of their content; see, e.g. Blogger removals, YouTube removals. Google keeps internal records of each appeal and the decision made. These notes are also used to better inform future decisions and retrain removal teams where needed.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles as well as recommended areas of improvement. A strength for Google is that the company has a creative and fluid approach to promoting the protection of freedom of expression and privacy, with multi-disciplinary, cross-functional teams considering human rights from local and global perspectives.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement.

Microsoft

The GNI Board conducted its third assessment review of Microsoft and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Microsoft is a global company that provides software, hardware, and cloud products and services to both enterprise and consumer customers. Its mission is to empower every person and organization on the planet to achieve more. The company employs some 135,000 personnel worldwide and operates subsidiaries in 131 countries. Its products and services range from the Windows operating system to the Azure cloud computing platform to the Surface line of tablet, laptop, and desktop computers.

This assessment focuses primarily on the impacts of Microsoft's consumer cloud services on the rights to freedom of expression and privacy. Examples of such services include Microsoft's Bing search engine, its LinkedIn professional social networking service, its Skype VOIP communications platform, its free Outlook.com webmail service, and its Windows Store, among others.

Microsoft

Governance

Microsoft's Board of Directors provides strategic oversight of the company's commitments, including to respect human rights, and the Regulatory and Public Policy Committee has primary oversight over GNI implementation. Day-to-day oversight of implementation of the GNI Principles is the responsibility of the VP and Deputy General Counsel who leads the human rights team within the Corporate, External and Legal Affairs (CELA) Department.

Microsoft's policy commitment to GNI is embodied in its public facing Global Human Rights Statement. Each business group is supported by a dedicated CELA team that provides frontline support on the full range of legal and public policy issues encountered in the development and delivery of products and services.

Due Diligence and Risk Management

Microsoft has due diligence processes to identify potential risks to the rights to privacy and freedom of expression that might arise from its business activities. The relationship between the company's business groups and the frontline CELA team that provides legal and public policy support is key to this process. Frontline personnel within each of its business groups who are most likely to encounter such issues identify and promptly report them to the CELA frontline team supporting them. Microsoft prioritizes among freedom of expression and privacy issues identified via due diligence based on salience, or in the case of positive impacts, its evaluation of where the potential to advance human rights is at its greatest.

Microsoft decides whether an HRIA is required based on the nature of the identified risks. These include the nature of the product or service under development, categories and quantities of data the service would require or generate, as well as the legal frameworks and human rights practices of the jurisdiction in question. Microsoft conducts HRIAs in-house, and also engages external experts to assist as warranted by the nature of the exercise.

Microsoft mitigates freedom of expression and privacy risks through a variety of means. This could involve design or other mitigation measures in the features or capabilities of a product, or in other cases adjusting or adapting the services or features offered in a given geography.

Freedom of Expression and Privacy in Practice

For government demands to restrict content, Microsoft requires a lawfully authorized legal order in writing (unless the applicable law allows oral orders) that is legally binding on Microsoft and complies with the rule of law. Microsoft attempts to comply with orders in a way that minimizes the impact on freedom of expression and provides information to users regarding generally applicable laws or legal demands requiring restrictions on content, and on Microsoft policies for responding to such demands.

Microsoft

The CELA law enforcement and national security team, and an analogous team at LinkedIn, is responsible for government requests for user data. Under the policy for handling such requests, Microsoft does not provide governments with direct and unfettered access to customer' data. Microsoft only pulls and then provides the specific data mandated by the relevant legal demand. Requests are reviewed to ensure they are valid, to reject those that are not, and to ensure only the data specified is provided.

Microsoft engages extensively with governments to advocate for the rule of law and the appropriate protection of all human rights.

To minimize and mitigate the risks associated with the collection, storage, and retention of personal information in the jurisdictions where it operates, Microsoft considers the nature of the services, the types of user data or content required to provide them, and the laws and human rights practices of each jurisdiction. Microsoft may adjust, adapt, limit, or avoid the operation of some types of services or features in certain jurisdictions. Microsoft requires third parties with whom it partners to provide its services to comply with the company's policies when it has operational control over them. This includes compliance with the company's policies and procedures to implement the GNI Principles.

Transparency and Engagement

Microsoft conveys its overall commitment to respect human rights through its Global Human Rights Statement and communicates its approach to emerging privacy and freedom of expression challenges through the "Microsoft on the Issues" blog. Microsoft communicates its GNI commitments to employees via internal policies, systems and procedures, and the provision of appropriate training.

Transparency reports, listed below, provide an overview of the company's policies and generally applicable laws and policies:

- Law Enforcement Requests Report
- U.S. National Security Orders Report
- Content Removal Requests Report
- LinkedIn's Transparency Report

The company's general practice is to provide users with notice if specific content has been blocked or removed in response to a government order unless prohibited by law.

Microsoft

Regarding *government orders* for content removal or user data, Microsoft is of the view that it is the role and responsibility of governments via judicial or other independent authorities to provide processes for appeals or other grievance mechanisms. Microsoft does provide its users with mechanisms to ask the company to reconsider content removal decisions pursuant to its Terms of Service. Microsoft also announced in May 2018 it would extend certain GDPR data subject rights to all customers worldwide.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. The main strengths include the degree of commitment at the highest levels of the company to implement the GNI Principles and the manner in which the company has integrated the GNI Principles into its operations, including the due diligence supported by frontline CELA teams.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement.

Millicom

The GNI Board conducted its first assessment review of Millicom and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Millicom International Cellular S.A. ("Millicom") is a provider of cable, fixed and mobile communications services that, during the assessment period, operated under the Tigo, Tigo Business, AirtelTigo, and Zantel brands in 11 countries across Africa and Latin America. The company is incorporated in Luxembourg, but the majority of its executive team is based in its U.S. office outside Miami, Florida. The company's shares are listed on the Nasdaq and Nasdaq Stockholm exchanges. Millicom offers a wide range of mobile and fixed services including mobile voice, data, and SMS; mobile financial services; high-speed wired Internet and cable TV; and an array of business solutions.

Millicom

Governance

Ultimate responsibility for Millicom's implementation of the GNI Principles rests with the company's General Counsel and its Chief External Affairs Officer. Operational responsibility for the development, implementation, and execution of policies and procedures rests with the company's legal team for the right to privacy, and with the Corporate Responsibility function of its External Affairs team for the right to freedom of expression. Millicom's Board of Directors receives updates on the company's implementation of the GNI Principles and its management of risks relating to the privacy and freedom of expression rights of its users at its quarterly meetings.

Due Diligence and Risk Management

Millicom incorporates human rights due diligence into its corporate due diligence and enterprise risk management processes. Millicom's Law Enforcement Response and Major Events Policy (LEA-MEP). is the company's key mechanism for empowering frontline personnel to escalate potential issues for due diligence, and ultimately, resolution. According to the policy, changes in a country's operating environment that materially increase the risks posed by Millicom's operations to the freedom of expression and privacy rights of its users are Major Events (see more below) that must immediately be reported to senior staff members. Under Millicom's LEA-MEP, members of its in-country Legal and Corporate Affairs teams are required to escalate to the company's senior-level executives proposed or actual changes in a country's surveillance as "Major Events."

Millicom prioritizes the human rights risks identified by its due diligence processes based on the severity and likelihood of impacts and its ability to mitigate those impacts, having due regard for the safety of its on-the-ground employees and the integrity and reliability of its operations. In 2017, Millicom engaged an external consultant to conduct an HRIA of Millicom's global operations (see "human rights impact and risk" in the 2017 LED Report). This exercise identified Millicom's most salient risks and laid out measures that the company could take across its operations to mitigate its potential adverse human rights impacts. Furthermore, the HRIA evaluated the legal and regulatory environment in each of the 11 countries in which Millicom operated at the time and identified future risk scenarios in those countries in the coming years.

The results of Millicom's HRIAs are incorporated into the company's business processes primarily through the work of its in-house Corporate Responsibility team. This team incorporates the learnings from HRIAs into the company's operations. The most important way in which Millicom mitigates the human rights risks its diligence processes identify is by creating robust systems to help its frontline, in-country personnel respond to government requests and demands.

Freedom of Expression and Privacy in Practice

Millicom's assessment of and response to government restrictions and demands that impact the privacy and freedom of expression rights of its users is directed by its LEA-MEP. Millicom draws a distinction between two categories of requests. The first is government requests for user data, which are issued in writing by an entity authorized under local

law to do so and appear on their face to be consistent with local law and international human rights standards. Such requests are logged in a database maintained by Millicom's in-country, in-house legal team that is audited by Millicom's corporate team on an annual basis. Millicom's in-country lawyers scrutinize such requests to ensure that they comply with all applicable local legal requirements. If they do, Millicom will grant the request on the narrowest possible basis. If not, Millicom will reject the request and explain its reasons for doing so to the requesting government entity.

The second category comprises all government requests and demands that are not in writing, obviously inconsistent with local law and/or international human rights norms or the terms of Millicom's operating license in that country or appear on their face to be politically motivated. These are considered "Major Events" that must be escalated to the company's executive-level personnel for review and decision. Once a Major Event is escalated to Millicom's senior personnel for their review and decision, the company evaluates the full range of available options before formulating a response. In so doing, the company attempts to balance its responsibility to respect international human rights norms with the practical reality of having to follow the local law in the countries where it operates.

Millicom limits access to the personal information it collects and retains regarding its customers and employees to those members of its staff who have a legitimate business reason to access such information. The company has devised information security measures and internal controls to prevent unauthorized access to such data, including the maintenance of logs that catalog all attempts to access such data, combined with periodic audits of these logs to ensure compliance.

Transparency and Engagement

Privacy and freedom of expression are together listed as Millicom's most important Corporate Responsibility topic in its most recent annual report, which also provides an overview of the company's approach and activities on these issues. More significantly, Millicom's extensive annual Law Enforcement Disclosure Report (LED Report) details the company's policies and procedures to protect the rights of its users in the face of specific government demands. In addition, a public version of the LEA-MEP was published in 2019.

In connection with the implementation of its Global Privacy Policy, Millicom is currently revamping its methods to notify customers' regarding the personal information it collects, and how it processes customers personal information, and to obtain their consent to such collection when necessary. As things stand, Millicom's local operations primarily inform their customers of their information collection practices through the contracts that are signed when they establish service. The websites of Millicom's local operations also include applicable Privacy Notices that detail the type of information the local operation collects from its customers and how such information is processed.

Millicom's LED Report also provides brief summaries of the legal frameworks of many of the countries under which it operates. The LED Report acknowledges that in several of these countries, "significant challenges exist with regards to the overall clarity of laws, legal oversight and separation of powers when it comes to laws around surveillance..." Millicom

highlights the availability of the GNI's Country Legal Frameworks Resource on its website and in its annual reporting, and commissioned the development of such reports for several of the countries where it operates.

Millicom has contracted an independent ethics hotline that is available to employees, customers, investors, and the public to report violations of the law or company policies, or to raise concerns about other forms of misconduct. Callers are afforded the opportunity to characterize their concerns as relating to "Data Privacy and Protection" or "Compliance with Laws and Regulations," among other areas.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. In particular, a main strength is that the LEA-MEP provides both specific and illustrative guidance as to the kinds of issues that local personnel must escalate to senior management, and provides a 24-hour "on call" system so that frontline employees know precisely to whom they should escalate a particular issue.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement.

Nokia

The GNI Board conducted its first assessment review of Nokia and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Nokia Corporation is one of the world's leading providers of mobile, fixed, optical, and IP-routing network infrastructure, which includes software, services, and technology hardware. The company employs over 100,000 people around the world and serves telecommunication network operators and vertical enterprise customers in 130 countries. Nokia supports a single network for digital services, converging mobile and fixed broadband, IP routing, and optical networks.

In addition to its communications network equipment business, Nokia also operates a successful patent and licensing business and conducts research and development through its Nokia Bell Labs organization. As of January 2019, the company comprises seven business groups: Mobile Networks, Fixed Networks, IP & Optical Networks, Global Services, Nokia Software, Nokia Enterprise, and Nokia Technologies.

Nokia was previously known for its mobile phone business. This business was sold in 2014. Nokia-branded phones and tablets available on the market today are created, marketed, sold, and supported by HMD Global Oy (HMD) — an independent company that is the exclusive global licensee of the Nokia brand for these purposes.

Nokia

Governance

Nokia's Board of Directors is responsible for overseeing the company's performance across a range of environmental, social, and governance topics. This includes Nokia's performance with regard to human rights issues — most notably in connection with the company's implementation of the GNI Principles.

Nokia's Group Human Rights Policy and its Code of Conduct form the basic structure through which the company implements the GNI Principles into its operations. The company has developed detailed internal Implementation Guidance to help operationalize the high-level commitments contained in the Group Human Rights Policy in specific circumstances. The Code of Conduct, meanwhile, summarizes the company's key human rights commitments and requires all employees to be on the lookout with regard to conducting business in high-risk countries, where the rule of law is weak. At an operational level, the most important way in which Nokia implements the GNI Principles is through its sales approval process. This is the process by which the company reviews all potential sales of its products and services against a wide range of considerations, including human rights risks.

Due Diligence and Risk Management

Nokia employs distinct mechanisms to identify the risks to the rights to freedom of expression and privacy associated with the sales of its products and services, the most significant of which is the company's sales approval process. This process includes a standard set of triggers to evaluate a potential transaction and various risk dimensions.

The main way in which Nokia mitigates risks related to freedom of expression or privacy identified by its due diligence processes is by unilaterally declining to sell certain of its products to customers located in countries where Nokia individually determines that its products are likely to be misused to interfere with these rights. Nokia uses an external risk rating company to assess country risks as one part of the input into this risk identification process. Given that for the most part Nokia does not sell individual pieces of equipment to its customers, but rather large packages of equipment required to enable a communications network, Nokia also considers whether it may supply its high-risk customers with certain network elements that pose a low risk of misuse, while withholding the sale of other network elements.

In other cases, Nokia considers whether its solutions can be customized to minimize the risk that its products will be misused to cause adverse human rights impacts. Minimization mechanisms that could be considered include limiting the personal information generated by or captured during the operation of a product and licensing the use of a software product as a separate item, as opposed to including it as a default feature.

Nokia

Freedom of Expression and Privacy in Practice

Nokia is an equipment vendor to providers of telecommunications services, rather than a service provider in its own right. Correspondingly, Nokia itself does not receive government requests to restrict content and turn over user data. Were Nokia to receive such requests from governments, it would be unable to fulfill them, as the company has neither the technical nor the legal ability to do so in view of the nature of its business.

At the time of the assessment, Nokia did not offer products or services for sale directly to individual end users. Correspondingly, Nokia does not collect or retain data about individuals in the manner that other companies must do in order to offer their products and services. Nonetheless, Nokia's Group Privacy Principles and its Privacy Management Policy commits the company to incorporate privacy by design into its products, and to minimize the collection and use of personal data.

Transparency and Engagement

Nokia communicates its general approach to addressing its human rights impacts in relation to freedom of expression and privacy by making its Group Human Rights Policy and Code of Conduct available online. In addition, the company publishes a People and Planet report every year that includes a section that details its approach to managing the privacy and freedom of expression-related risks of its business. Since 2017, the People and Planet report has included anonymized summaries of human rights due diligence cases reviewed by the company in the previous year. Nokia also reports on human rights issues in its annual Form 20F filed with the U.S. Securities and Exchange Commission. In addition, Nokia uses a variety of communication channels to communicate its approach to human rights to external and internal stakeholders — including blog posts, internal and external social media channels, and company participation in regional and global human rights gatherings and events.

Nokia does not have any "users" in the sense that this word is typically used in the GNI assessment context, as the company's customers are overwhelmingly other businesses. That said, Nokia's Privacy Statement governs the company's collection, storage, and use of personal information for its business purposes (including employee-related information).

Nokia employees and external stakeholders alike can report violations of the Company's Code of Conduct and related Group-level policies using Nokia's dedicated 24-hour ethics hotline. Such reports can be filed anonymously. In addition, Nokia employees can report any concerns they may have to the company's global Ombuds program.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement.

Nokia

Nokia is the first vendor whose compliance with the GNI Principles has been assessed. Because vendors typically do not have in their possession the type of content sought by law enforcement or government agencies, nor do they control the networks censored by governments, many of the mechanisms called for in the GNI Implementation Guidelines are simply inapplicable to Nokia's operations. Nokia, its assessor, and the GNI Board, all recognized this. For Nokia, it was particularly important that human rights triggers were built into its sales approval process. The incorporation of human rights due diligence into this core business processes provides assurance that transactions which may pose significant human rights impacts are not escaping the attention of Nokia's human rights team.

> "Nokia sets great store by our commitment to human rights — throughout our entire operations, from supply chain and workplace, to ways in which our technology is used. So, we are proud to be the first communications equipment vendor to have joined GNI as a board member and to be assessed under its rigorous standards. We are pleased with the positive outcome and look forward to our continued engagement with the GNI community."
>
> FIONA CURA-PITRE, Nokia

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement. For Nokia, one example of an assessor recommendation is to consider developing a formal business process for evaluating the human rights risks and opportunities presented by the innovative technologies it is developing, such as 5G and artificial intelligence, with a view of better informing the due diligence it will conduct prior to the sale of such technologies in the future.

Orange

The GNI Board conducted its first assessment review of Orange and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Orange is one of the world's leading telecommunications operators with revenue of 41 billion euros and 151,000 employees worldwide, including 92,000 in France, by the end of 2018. The Group served 264 million customers in 2018 (204 million mobile customers and 20 million fixed broadband customers). With presence in 27 countries, Orange is also a leading provider of telecommunication services to multinational companies, under the brand Orange Business Services. Orange SA is the parent company of the Orange group and carries the bulk of the Group's activities in France. Orange has been listed since 1997 on Euronext Paris and on the New York Stock Exchange (NYSE).

Orange

Governance

In 2017, France passed legislation regarding "Le Devoir de Vigilance" or "Duty of Vigilance" for corporate actors to guard against negative human rights impacts of their business decisions. Orange Group was required by this law to develop and implement a vigilance plan, which includes reasonable oversight mechanisms to identify risks and prevent serious abuses of human rights and fundamental freedoms derived from the company's activities. It includes a risk map, procedures for evaluating the position of subsidiaries, subcontractors and suppliers, actions adapted to mitigating risks or the prevention of serious abuses, an alert mechanism (whistleblowing system), and a mechanism for the collection of reports, as well as a system for monitoring the measures taken.

> "The GNI assessment has strengthened our Vigilance Plan to follow up on government demands."
>
> YVES NISSIM, Orange

The GNI Principles have been integrated into the Group policies via the Vigilance Plan, which compiles several processes that meet the requirements of a number of GNI Principles. The specific Human Rights and Fundamental Freedom risk as well as Health and Safety risk and Environmental risk have been raised to the highest level of Board oversight. Risk of breaching human rights and fundamental freedoms has thus been identified by Orange as a Group non-financial risk under its risk management and internal control system, which consists of an organizational structure, procedures, and control systems implemented by senior management and all employees under the responsibility of the Board of Directors.

Due Diligence and Risk Management

In addition to the Vigilance Plan described above, the Group's management teams identify and assess, at least once a year, the risks falling within their remit. Risk mapping also includes a description of action plans designed to address these risks by strengthening internal control. The list of significant events, the changes to risk mapping, and the monitoring of action plans are scrutinized during internal control reviews. At Group level, risks are monitored by the Group Executive Committee's Risk Committee. The overall Risk Management Report is reviewed at least once a year by the Risk Committee and presented to the Directors at a Joint Committee of Board Committees, during which major risks are discussed in the presence of the directors concerned. Orange has recognized at Group level that the company is exposed to risks of disclosure or inappropriate modification of personal data, in particular customer data, affecting privacy.

Orange

Orange has identified the risk to privacy as a core risk, incorporating privacy in its Time to Market process linked to the development of new products or upgraded products. Moreover, Orange has defined the risk to freedom of expression and privacy in its risk assessment matrix as part of its Vigilance plan.

Risk analysis is the major tool used to determine if a human rights impact assessment is necessary. Orange uses Verisk Maplecroft, a specialist external firm using a methodology based on UN and OECD standards, to carry out a customized assessment of the risks incurred in terms of compliance with human rights in each country where Orange operates, to assess and target its actions. On top of Verisk Maplecroft analysis, Orange tracks governmental requests or demands with potentially serious impacts on freedom of expression, and against an electoral calendar to anticipate possible concerns.

Freedom of Expression and Privacy in Practice

Orange's policies and procedures for responding to government restrictions and demands are captured in the document "Process to be followed in advent of a major infringement on freedom of expression," which covers the specific components of the GNI Implementation Guidelines.

Monitoring the management of the Personal Data Protection governance program is undertaken by both the Group Security Department and the Personal Data and Security Department of the Group's Legal Department. The approach taken by the Group Security Department is audited by a yearly assessment to check compliance with the Group's Security Standard.

Transparency and Engagement

Orange communicates its human rights impacts in relation to freedom of expression and privacy via various channels to shareholders and stakeholders:

- Annual report on freedom of expression
- Orange vigilance plan
- Document on implementation of the GNI Principles
- A booklet on Orange's policies regarding human rights
- A dedicated website on personal data protection

Orange offers grievance mechanisms to its customers. For example, in France, there is a link to a postal address and a link to a downloadable form for enterprise customers, a postal address and an Internet access path for residential customers, and an external appeal to the authorities CNIL (French National Commission of Computing and Freedoms) at Group level. Orange also offers a whistleblowing mechanism for grievances, including related to personal data, via an email address.

Orange

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. One strength is the integration of freedom of expression and privacy into the company's overall Vigilance Plan, with well-defined roles within the company and an internal structure for risk management that involves local subsidiaries while requiring internal guidelines to be followed.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement. For Orange, an example of an assessor recommendation is to publish in its integrated annual report information on its fight for freedom of expression and the protection of personal data. Successful cases could illustrate this commitment, as long as employee safety is not put at risk.

Telefónica

The GNI Board conducted its first assessment review of Telefónica and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Telefónica's business model is based on four platforms:

1. Physical assets from networks and base stations to stores or customer equipment.
2. IT & Systems that contain support and commercial systems.
3. Product and services such as video, cloud, big data and security as well as aggregate third party services.
4. Cognitive power that aims to help create better experiences for customers using artificial intelligence tools.

The company is organized across the following segments: Telefónica Spain, Telefónica United Kingdom, Telefónica Germany, Telefónica Brazil, Telefónica Hispam Norte (Central America, Colombia, Ecuador, Mexico, and Venezuela) and Telefónica Hispam Sur (Argentina, Chile, Peru, and Uruguay). Telefónica also has Telxius, a telecommunications infrastructure company that manages more than 16,550 towers of high-capacity optic fiber cable network.

Telefónica

Governance

The GNI Principles are implemented at Telefónica via the Responsible Business Plan, which is approved by the Board of Directors and defines the company's sustainability objectives, including commitments to privacy and freedom of expression. The senior-directed human rights function is held by the Global Director of Corporate Ethics and Sustainability, who designs, coordinates and leads the implementation of the GNI Principles. The Responsible Business Plan helps ensure that the commitments laid out in the GNI Principles are incorporated into routine business operations. The involvement of the department heads in the Responsible Business Office ensures that topics such as privacy and freedom of expression are adequately communicated to employees working in the respective areas.

Due Diligence and Risk Management

Telefónica has a human rights due diligence process in place to identify, prevent, mitigate and account for human rights risks in general and risks to privacy rights and freedom of expression in particular. An integral part of this process are human rights impact assessments, which are conducted every four years. The latest human rights impact assessment in 2017/2018 identified privacy and freedom of expression as one potential area of human rights impact. Telefónica also conducts more specialized human rights impact assessments, both on a product and market-level.

Telefónica evaluates possible human rights impacts of new products and services via a "human rights by-design-approach," which the company is currently implementing. In this approach, product managers conduct a self-assessment via an online tool in the design phase of new products and services with a view to identifying and addressing potential adverse effects already at this stage.

Once (actual or potential) risks to the freedom of expression and privacy rights are identified in the due diligence processes elaborated on above, Telefónica acts upon these findings and adapts internal policies and processes accordingly. For example, human rights were integrated as a specific risk in Enterprise Risk Management so that risks arising out of substantial changes in existing products and services are also raised and addressed.

Freedom of Expression and Privacy in Practice

In 2016, Telefónica adopted a "Global Rule on Requests made by Competent Authorities" (hereafter "Global Rule"), which sets out how all companies within the Group are to assess and respond to requests made by competent authorities in relation to:

1. the lawful interception of communications,
2. the provision of metadata associated with communications,
3. blocking of websites, and/or restriction of certain content, and
4. suspension of networks or services.

Telefónica

This Global Rule ensures compliance with legal obligations vis-á-vis the competent authorities in the respective countries, while protecting at the same time the fundamental rights of the people affected. It was elaborated in accordance with the principles of the former Telecommunications Industry Dialogue and updated based on the GNI Principles and learnings within the GNI community.

The Global Privacy Policy of Telefónica, which was updated in 2018, establishes a set of mandatory rules that all companies within the Group are to follow to minimize and mitigate the risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate.

Transparency and Engagement

Telefónica communicates its human rights impacts in relation to freedom of expression and privacy via various channels to shareholders and stakeholders:

- The annual management report of Telefónica integrates relevant non-financial information. It contains a separate chapter on human rights and repeatedly stresses the company's commitment to privacy rights and freedom of expression in general and the GNI Principles in particular.
- The Consolidated Management Report is meant to reach not only company´s shareholders, but also its stakeholders in its entirety. For this purpose, the sections on human rights, privacy, freedom of expression, and the GNI Principles, respectively, are elaborated on in even greater detail.
- Telefónica publishes a yearly Transparency Report related to requests from competent authorities regarding legal interceptions, access to metadata, blocking and filtering of contents as well as suspension for services.
- The Telefónica website provides further information on the company's approach to sustainability, in general, and human rights/privacy and freedom of expression, in particular, with a view to making this information publicly available to all interested stakeholders. Instrumental in this respect are Privacy Centers that serve as a one-stop-shop for stakeholders (particularly customers) interested in knowing more about Telefónica's approach to privacy and freedom of expression.
- Telefónica has an institutionalized dialogue with its stakeholders via the Telefónica Stakeholder Panel and proactively engages with investors/analysts on environmental, social and governance (ESG) topics.
- Telefónica discloses what personal information it collects, via its Global Privacy Policy. Telefónica also has a Privacy and Security Centre, where customers can find relevant information on privacy and security matters.
- The company's policies and procedures for responding to restrictions and demands by competent authorities are explained in Telefónica's Transparency Report. The relevant procedure in this respect is in the "Global Rule," a summary of which is also publicly available.

Telefónica

With its Responsible Business Channel, Telefónica has a mechanism in place that allows stakeholders, in general, and users, in particular, to make grievances about issues related to freedom of expression and privacy and, if appropriate, receive remediation. To be more precise, grievances can be made in relation to various categories, two of them being freedom of expression and privacy. The concrete procedure and the principles governing the processing of said grievances are explained in detail in the publicly available Group Regulation about the Management of the Business Principles Channel.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. A main strength is that the company had adopted policies and procedures, which outline how they shall assess and respond to government demands in relation to restriction to communications, protect privacy, and allow freedom of expression.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement. For Telefónica, one example of an assessor recommendation is that the company consider providing specific training for those corporate employees who are most likely to have to address freedom of expression matters and providing a specific training for senior management and the board that facilitates deeper reflection on future challenges in the application of the GNI Principles.

Telenor Group

The GNI Board conducted its first assessment review of Telenor and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Telenor Group is an international provider of tele, data, and media communication services. In the assessment period, Telenor had mobile operations in the following markets:

WHOLLY OWNED	WHOLLY-OWNED — SUBSIDIARY	SHAREHOLDER
Norway	Denmark	dtac
	Sweden	Thailand (minority)
	Pakistan	DiGi
	Myanmar	Malaysia (minority)
	Hungary	Grameenphone
	Bulgaria	Bangladesh (majority)
	Montenegro	
	Serbia	

Telenor Group

Governance

The assessment explored how Telenor's Board of Directors approves the company's human rights policies and exercises oversight with the support of its Sustainability and Compliance Committee. The GNI Principles are implemented through the Authority Requests Manual, which provides mandatory requirements for handling government requests across Telenor's business units. At the business unit level, experts from privacy, legal, sustainability, security, communications, and public and regulatory affairs will assess challenging cases and escalate if needed to the business unit CEO. A point of contact at the Group level (Group Single Point of Contact — SPOC), responsible for privacy, engages with the business units on these issues, receives the escalations, and will summon a Group level team representing the same functions as the local escalation team as required.[24] For any cases that are particularly challenging or of high risk, this team will escalate the request to a high-level steering committee to make a decision, in collaboration with the business unit CEO. If the request cannot be resolved at this level, Group CEO will decide on necessary actions. In addition, business units undergo periodic assessments of the authority request manual implementation.

Due Diligence and Risk Management

Telenor employs an ongoing process of human rights due diligence to identify, prevent, mitigate, and account for human rights impacts, in alignment with the UNGPs. This is set out in the Group Sustainability Policy and is mandatory at Group and business unit level. Privacy and freedom of expression were identified as salient issues in a 2017 Group-level mapping exercise, and a Human Rights Due Diligence Toolkit provides guidance for implementation.

Due diligence is conducted regularly; the frequency is determined by the market and level of risk. When authority requests require rapid response, Telenor has developed a Rapid HRDD Template which was piloted in 2018/2019. Telenor has specific due diligence actions for different activities:

- Products: Telenor takes a risk-based approach in any kind of data processing.
- Markets: Prior to entering Myanmar, the company conducted a HRIA as part of due diligence and reports progress on key findings in annual sustainability briefings.
- Acquisitions and partnerships: Due diligence is exercised before engaging with third parties, as outlined through a Group policy on third party risk.
- Other business relationships: Respect for human rights and privacy is included in Supplier Conduct Principles.

Telenor's human rights prioritization is based on the analysis of the severity of the risk to define group-wide salient issues. Such risks are also considered as part of a holistic assessment that includes legal and security risks.

[24] To ensure Group involvement at an earlier stage of the escalation process, Telenor has since revised its AR Manual to require escalation to business unit CEO and Group SPOC simultaneously.

Freedom of Expression and Privacy in Practice

Telenor's Authority Requests Manual was updated in the reporting period based on learnings, best practices identified from other companies, and the formulations found in the GNI Principles. Per the Authority Requests Manual, business units implement routines for checking that authority requests meet procedural and material requirements for a valid legal basis under local law. When requests lack a clear legal basis or pose a significant risk of serious human rights impact, business units shall inform the authority accordingly and refrain from executing the request, to the extent reasonably possible without risking disproportionate reprisals. The updated manual, which came into effect in August 2018, specifies that requests and legal basis shall be interpreted as narrowly as possible.

Business units are expected to engae with the authorities in accordance with guidelines and on a regular basis. A checklist was developed to help execute these responsibilities. In the Spring of 2018, a Checklist for Authority Request and Business Environment Management was developed to help business units execute on these responsibilities.[25] The Public and Regulatory Affairs unit, at both Group and business unit levels, engages authorities regularly. Telenor may also submit input to proposed legislation, encourage legal frameworks that meet international standards, and engage in international policy discussions.

The company-wide Privacy Policy and Manual includes the following key principles:

- Personal data should solely be used for the purposes for which it was collected, with a valid legal basis for processing
- Each business unit has a designated Data Protection Officer
- Each business unit is required to conduct Data Protection Impact Assessment (DPIA), and other measures to keep data secure

In addition, Telenor has a data breach manual.

Transparency and Engagement

Telenor publishes an Annual Sustainability Report as well as information on its website including transparency reports, a legal frameworks overview, and historic reports on the Telecommunications Industry Dialogue. Group and business units engage with shareholders and stakeholders through regular meetings and events. For example, Telenor Myanmar hosts an annual Sustainability Forum, a multistakeholder gathering where they report on the progress related to a number of risks including freedom of expression and right to privacy. The Group CEO has also spoken publicly on these issues. GNI commitments are communicated to employees through an intranet site.

[25] This is now called the BU Authority Request Action Plan.

Telenor discloses to users what personal information the company collects through the privacy notice for each company. For example, see Telenor Pakistan Privacy Notice. A dedicated "Handling Access Requests from Authorities" page and legal overviews of laws related to freedom of expression/privacy for all operating markets disclose both the generally applicable laws and policies, which require the company to restrict content or communications or provide personal information to government authorities, and the company's policies and procedures for responding to government restrictions and demands.

The main mechanism for reporting grievances is the Integrity Hotline, which is available to anyone with the option to anonymously report suspected breaches of the company Code of Conduct, which includes grievances related to freedom of expression and privacy. In practice, more day-to-day questions about these issues come through customer service channels. During the reporting period, no grievances were reported that related to the GNI Principles.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. The assessment showed that Telenor is evaluating and improving its efforts to implement the Principles. For example, Telenor has developed a set of continuously updated manuals for those engaged with authority requests, as well as tools for HRIA and HRDD.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement. For Telenor, an example of a recommendation to further optimize its systems is to consider centralizing its systems to track its policy implementation and understand the number of government requests it receives that fall outside acceptable standards.

Telia Company

The GNI Board conducted its first assessment review of Telia Company and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Telia Company provides:

- Mobile voice and data
- Fixed voice and data
- IP capacity
- TV and media

Telia Company's operations also include the following lines of business: Carrier, 'Division X,' Analytics, and Cygate, which is a leading provider of integrated solutions to business customers in the Nordics.[26]

Telia Company has its roots in Finland and Sweden. Home markets today are the Nordic and Baltic countries. During 2015, Telia Company announced the decision to exit Eurasia, enabling it to fully focus on the core markets and strategy as New Generation Telco. As of June 2018, Telia Company still owned operations in Kazakhstan (Kcell), Moldova (Moldcell), and Uzbekistan (Ucell), as well as a minority share in Turkcell (Turkey). Telia Company had divested its operations in Nepal (December 2015), Tajikistan (April 2017), Georgia (January 2018) and Azerbaijan (March 2018) as well as its minority ownership in MegaFon (Russia) (October 2017). Within Telia Company, each country organization is responsible for running the operations. Telia Company's backbone fiber, Telia Carrier, runs around the world and is the second largest in the world, with wholesale customers in more than 110 countries.

[26] Since December 2019 Telia Company owns Bonnier Broadcasting and thus includes a Broadcasting unit.

Telia Company

Governance

At Telia Company, implementation of the GNI Principles primarily occurs via the company's policy on freedom of expression & surveillance privacy. This policy is owned by a group function, with dedicated roles for other members of senior management, and is reapproved annually by Telia Company's Board of Directors after a preparatory review by the relevant board committee.[27] Freedom of expression and surveillance privacy risks related to Telia Company's operations are reviewed in a manner consistent with Telia Company's overall approach to risk management through the Governance, Risk, Ethics, and Compliance (GREC) forum. GREC meetings are held at both the group and country levels. In addition, a Group Level Human Rights Virtual Team facilitates policy coordination, shared learning, analysis, business integration, and alignment on human rights.

Due Diligence and Risk Management

Telia Company follows several processes to identify risks to freedom of expression and privacy. These include GREC, the company's seven responsible business focus areas, its risk management process, and the HRIAs conducted for eight markets and performed by BSR, an independent nonprofit organization. The company is also committed to undertaking some form of HRIA, including on freedom of expression and surveillance privacy, as appropriate.

Where Telia Company does have operational control, the Policy and Instruction on Freedom of Expression & Surveillance Privacy applies fully. Where Telia Company does not have operational control, the policy states: "Telia Company works toward promoting and adopting this Policy's principles and objectives in other associated companies where Telia Company does not have control but has significant influence."

Telia Company's responsible business focus areas, including the one on freedom of expression and surveillance privacy, provide a structure and governance for ongoing due diligence. The respective responsible business focus area owner provides group-level advice and support, based on the company's policy and instruction.

The Telia Company Group Policy on Freedom of Expression & Surveillance Privacy establishes how local companies and other units assess and escalate unconventional government requests or demands. The policy, adhering Instruction, and guidance in the Form for assessments and escalation, provides the process for prevention and mitigation of freedom of expression and surveillance privacy risks in relation to unconventional requests. The definition of "requests" include significant or proposed changes in the law, or significant imposed or proposed operational changes, in this context.

Freedom of Expression and Privacy in Practice

The Telia Company Group Policy on Freedom of Expression & Surveillance Privacy describes how the company will assess and respond to government requests and demands. In addition to the publicly available policy, an instruction

[27] Due to changes since the completion of the assessment this policy is now owned by Group People & Brand Group Sustainability.

Telia Company

sets out how the policy is implemented, including steps requiring governments to follow established domestic legal processes, requesting clear written communications, and soliciting the narrow interpretation of government requests.

Telia Company has, in connection with the implementation of the privacy legislation GDPR in May 2018, thoroughly assessed all collection, storage, and retention of personal information in Telia Company's markets within the EU adding also operations in Norway. Telia Company has reviewed internal processes, privacy policies, and security measures, trained staff, and made necessary changes in IT-systems to enable customers to exercise their right to access data deriving from GDPR.

Transparency and Engagement

Telia Company communicates its commitment to the GNI Principles through formal public reporting (including law enforcement disclosure reporting and annual and sustainability reporting), public communications (including statements, policies, and articles), and informal engagement through regulatory and public affairs activities.

Telia Company has drafted Privacy Policies for its different companies, products, and services that contain information about what personal data the company processes. The Privacy Policies are provided to customers at the time of onboarding and are publicly available on Telia Company websites. Surveillance laws are disclosed to users mainly through the Telia Company Law Enforcement Disclosure Reports (full reports are issued every March and statistics updates every October). The reports include context about surveillance legislation, a list and statistics on conventional as well as unconventional requests, and links to laws on direct access and on data retention. Regarding direct access, Telia Company also explicitly highlights that it does not know the amount of surveillance and cannot provide statistics. Telia Company has published its Policy and has a public version of the Form for assessments and escalation.

Telia Company has set up a whistle-blowing tool, the Speak-Up+ Line, which allows for human rights issues to be raised, including freedom of expression and surveillance privacy. The system is also available for external stakeholders.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. Within the senior management team of Telia Company, the assessor observed that careful attention was paid to unconventional requests and demands from authorities in the countries where Telia Company operates.

See Section 3 for an overview of recommendations made by assessors to one or more companies for improvement. An example of an assessor recommendation for improvement was that Telia Company considers implementing a formalized process to identify potential risks related to freedom of expression and privacy that may be connected to its products. This may be usefully incorporated into the existing risk assessment processes for when new products are developed.

Verizon Media

The GNI Board conducted its assessment review of Verizon Media and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time. This is the third GNI assessment of Verizon Media, previously Yahoo, a founding member of GNI.

The Company

Verizon Media houses a dynamic set of global media and technology brands, including two of the Internet's most recognized brands: Yahoo and AOL. Yahoo, a founding member and Board member of the GNI, was acquired by Verizon, Inc. ("Verizon") and joined with AOL, Inc. ("AOL") to form Verizon Media (formerly Oath) in 2017. Verizon Media provides consumers with owned and operated search properties and finance, news, sports and entertainment offerings; and provides digital advertising platforms.

Verizon Media

Governance

The Business and Human Rights Program (BHRP) is a team of senior human rights professionals within the company within the company responsible for leading efforts to make responsible decisions with respect to human rights, particularly freedom of expression and privacy.

The BHRP, under the remit of the General Counsel, has primary responsibility for driving Verizon Media's implementation of the GNI Principles. The BHRP works with a global virtual, cross-functional team consisting of senior employees and experts from across the company to integrate human rights considerations in business decision-making processes within Verizon Media. The Corporate Governance and Policy Committee of the Verizon Board of Directors receives periodic updates about global human rights risks and opportunities related to Verizon Media.

Due Diligence and Risk Management

The BHRP designs and implements ongoing human rights due diligence policies and procedures to identify human rights risks and opportunities related to Verizon Media's business decisions. This includes the preparation of human rights impact assessments (HRIAs) of decisions related to the company's operations, products, or services. The BHRP has published information about its process for human rights due diligence on its website.

Freedom of Expression and Privacy in Practice

Verizon Media has published Global Principles for Responding to Government Requests for content removal and for user data — informed by the GNI Principles. The cases reviewed by the assessors and considered by the GNI Board provided evidence that these Principles are followed in practice in Verizon Media's process for responding to government requests. This includes showing that the company requires clarification of requests, demonstrates willingness to challenge requests when necessary, and has developed escalation procedures for appropriate circumstances. In addition, Verizon Media considers risks associated with the collection, storage, and retention of personal information as part of assessing the human rights impacts of its business decisions.

Verizon Media's Global Public Policy team, working in collaboration with the BHRP, leads engagement with governments around the world to advocate for the rule of law and respect for privacy and freedom of expression.

Transparency and Engagement

The BHRP website is part of Verizon Media's main corporate website and articulates the company's approach to business and human rights, which builds on Yahoo's pioneering programmatic work. The BHRP maintains a public-facing blog on this website.

Verizon Media has also published a Transparency Reporting Hub that contains information about how the company puts its commitment to its users into action. It discusses the BHRP and Verizon Media's membership in GNI, as well as

Verizon Media

Verizon Media's Global Principles for Responding to Government Requests. It also contains a FAQ section that provides information on Verizon Media's approach to responding to government demands.

Importantly, the Hub houses Verizon Media's Government Requests Transparency Reports with information on government requests for user data, including national security requests for user information in the United States, to the extent allowed by U.S. law. The report also contains information on government requests for content removal. Verizon Media provides illustrative examples of the type of requests it receives and how it responds to those requests. This includes all requests it identifies as coming from a government agency, including government requests to remove content based on Verizon Media's Terms of Service or Community Guidelines.

Verizon Media further communicates with users through its Terms of Service and Privacy Policy. The company has also developed a microsite that explains how and when user data is collected and used and provides users with a personalized privacy dashboard.

Verizon Media may notify users via email when user-generated content is removed or blocked. Verizon Media notifies users about third party requests for their information prior to disclosure. This provides users with an opportunity to challenge the request. There may be instances where notice would not be provided to a user. For instance, where the company is prohibited by law from providing such notice, or where there is an imminent threat of physical harm to a person in an emergency situation. Steps are taken to provide delayed notice to the affected user when possible.

Information about Verizon Media's whistleblower channel, including a link to make reports via "The Network," a third-party compliance reporting website, is provided in the company's Standards of Business Conduct, which states that the company considers human rights in its business actions and decisions. The BHRP also makes its email address publicly available so that anyone can contact the BHRP about issues related to Verizon Media's global human rights commitments.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. Following Yahoo's acquisition and the formation of Verizon Media encompassing Yahoo and AOL, the BHRP was charged with leading efforts to inform responsible decision-making on important human rights issues of freedom of expression and privacy across the entire company. This demonstrated the importance that Verizon Media's leadership attaches to human rights issues. The assessor reported on Verizon Media's progress against recommendations made from the prior 2015/2016 assessment and noted that significant progress was made.

See Section 3 for an overview of recommendations made in the 2018/2019 assessment cycle by assessors to one or more companies.

Vodafone Group

The GNI Board conducted its first assessment review of Vodafone Group and determined the company is making good-faith efforts to implement the GNI Principles with improvement over time.

The Company

Vodafone Group is one of the world's leading telecoms and technology service providers. Vodafone Group has extensive experience in connectivity, convergence and the Internet of Things, as well as championing mobile financial services and digital transformation in emerging markets.

Vodafone Group has mobile operations in 24 countries, partners with mobile networks in 41 more, and fixed broadband operations in 19 markets. As of September 30th, 2019, Vodafone Group had approximately 625 million mobile customers, 27 million fixed broadband customers and 22 million TV customers, including all of the customers in Vodafone Group's joint ventures and associates.

Vodafone Group offers a wide range of products and services and aims to provide a unified experience to its customers combining mobile, fixed voice, broadband, TV and other services. Vodafone Group also offers mobile, fixed and a suite of converged communication services to support the needs of its Enterprise customers, who range from small businesses to large multinational companies.

Vodafone Group

Governance

The Vodafone Group External Affairs Director is the most senior representative with responsibility for the GNI Principles and is a member of the Vodafone Group Executive Committee.[28] The Executive Committee exercises oversight of the implementation of the GNI Principles through sponsorship of policies, receiving reports, the use of subcommittees as part of overall company due diligence and governance activities, and consultation and sign off on external stakeholder engagement and GNI engagement on human rights issues. Within senior management, the sustainable business team has lead responsibility for implementation of the GNI Principles with other teams, including, but not limited to, security, privacy, and policy. These teams work closely with their local market counterparts. The GNI Principles are integrated into routine business operations, through Group policies and implementation guidelines, risk mitigation processes, governance, ongoing monitoring, and reporting and transparency.

Due Diligence and Risk Management

Vodafone Group's approach is to embed a human rights risk assessment into the due diligence investigation for new and upcoming products and markets. This is achieved by ensuring each step of the risk assessment process is contained within the due diligence investigation.

Freedom of Expression and Privacy in Practice

Vodafone Group has a law enforcement assistance policy, which outlines the governance and safeguards the company has in place to ensure it balances respect for its customers' rights to privacy and freedom of expression with its legal obligations to support a free and secure society.

Vodafone's Customer Privacy Portal and Report explains how the company's privacy policies and a framework governs the collection, use, and management of customer information. Protection of personal data is central to the Vodafone Code of Conduct. In some instances, Vodafone has taken steps beyond what is required for legal compliance, to minimize and mitigate the risks associated with the collection, storage, and retention of personal information wherever they operate.

Transparency and Engagement

Vodafone Group publicly reports its freedom of expression and privacy impacts through several means, including the Digital Rights and Freedoms Portal, the Annual Sustainable Business Report, and the Vodafone Group Annual Report.

The Digital Rights and Freedom Portal includes the Law Enforcement Assistance Disclosure Statement and the Legal Annex (with overviews of powers in each market). The company also publishes a country-by-country disclosure of demands made on the company.

[28] Vodafone Group's operational leadership team is referred to as an "Executive Committee" instead of "Board."

Vodafone Group

Freedom of expression and privacy complaints can be made via Vodafone Group's normal customer service channels, from where they are then routed to the responsible organizations and teams. Privacy queries can be submitted to a dedicated site for specific local markets. General enquiries from external stakeholders on freedom of expression and privacy are made through media lines or directly to the sustainability team. Customers can use Vodafone Group's customer service channels.

Follow Up and Improvement

The GNI Board took note of the assessors' views on the company's main strengths and successes in implementing the GNI Principles, as well as recommended areas of improvement. For Vodafone Group, the assessor noted that the GNI Principles are also well understood and embraced by senior leaders in a number of key areas of the business and that the company uses technology and existing compliance systems to embed human rights into everyday company procedures and processes.

See Section 3 for an overview of recommendations made in the 2018/2019 assessment cycle by assessors to one or more companies.

3) Improvement Over Time

3) Improvement Over Time

Continuous improvement is a critical component of GNI's approach to freedom of expression and privacy. As the GNI Principles state, "while infringement on freedom of expression and privacy are not new concerns, the violation of these rights in the context of the growing use of ICT is new, global, complex and constantly evolving." This is why the GNI Board focuses on whether a company is making good-faith efforts to implement the GNI Principles with improvement over time. Each company's assessment report, including the process review and case studies, is designed to show how companies have evolved their policies and procedures and their approach to freedom of expression and privacy rights during the assessment period.

Assessor recommendations to companies are also an avenue for improvement over time. Companies are not required to adopt the assessor's recommendations. Rather, each recommendation provides the company an opportunity to review the issues or questions underlying the recommendation and determine what actions or changes (if any) to undertake (which may be different from the assessor's recommendations). In each subsequent assessment, the GNI Board reviews recommendations made during the prior assessment of each company and the actions or changes undertaken (if any) by the company. Assessors are asked to explain whether a company has implemented a recommendation, is in the process of implementing it, or has decided not to implement the recommendation as suggested, but has chosen to address the specific issue in another way.[29] The GNI Board considers these explanations in the context of its good-faith determination.[30]

Based on a review of the assessment materials, the GNI Board may make recommendations to a company regarding alternative approaches to the implementation of the GNI Principles. If the company modifies (i.e., takes steps to address the concern that prompted the recommendation that differ from the actions the board recommended) or rejects a recommendation, it will explain its decision to the GNI Board in its next assessment. Board recommendations are approved by a majority vote of the board other than board members representing the company being assessed. Recommendations from individual board members constitute "informal feedback" to the company and do not trigger a mandatory response from the company.[31]

During this assessment cycle, the GNI Board made a total of five recommendations to four companies.

[29] See Question 6.4 in the Process Review Questions in Appendix I of the Assessment Toolkit.

[30] According to Appendix V of the Assessment Toolkit, Process Description for Board Review Meeting: "Engagement with recommended steps in a prior assessment shall be considered as an important factor by the Board in concluding whether the GNI member company is making good-faith efforts to implement the Principles with improvement over time."

[31] The focus of the board review is to assess company members processes. The GNI Board does not comment on or make recommendations regarding a company's business decisions, its specific business criteria, or its business terms of dealing. Companies always remain free to conduct business unilaterally, as they determine what is in their individual best interest. The focus of the board's formal and informal recommendations, and other engagement, is on the assessed company members' processes and do not comment on or intend to comment on members' business decisions or terms of dealing.

Recommendations to Companies

Assessors made 70 recommendations for improvement to the 11 assessed companies, according to the categories from the Assessment Toolkit:

ASPECT OF ASSESSMENT	NUMBER OF RECOMMENDATIONS
Context of Assessment	3
Governance	29
Board Oversight	1
Escalation	1
Internal Structures	10
Training	13
Senior Management	4
Due Diligence and Risk Management	17
Divestment	2
Due Diligence	5
Human Rights Impact Assessments	4
Other Business Relationships	2
Suppliers	1
Risk management	3
Freedom of Expression and Privacy in Practice	8
Policies and Procedures	4
Seeking Assistance	1
User Data Requests	3
Transparency and Engagement	13
Transparency Reporting	2
Communication with Users	1
Engagement with Governments	4
Engagement with Rightsholders	1
Grievance Mechanisms	1
Internal Communications	4

"GNI assessments provide a unique mechanism for human rights groups to examine the policies and procedures companies have to government censorship and surveillance demands to assess whether companies are putting GNI Principles into practice and improving their performance over time."

ARVIND GANESAN, Human Rights Watch

The following are examples of recommendations made by the independent assessors for companies to consider, based on findings from the current assessment cycle. Some recommendations are generalized.

Context of Assessment

- Several recommendations concerned suggested changes to company practices to better prepare for and enable future assessments.

Governance

Recommendations to consider under governance, include:

- Preparing and facilitating dedicated briefing sessions or reports for new Chief Executive Officers and/or other senior management on company efforts related to implementing the GNI Principles.
- Ensuring policies and procedures relating to the GNI Principles are consistently applied across all company products or business units, including recently acquired companies.
- Formalizing reporting processes on issues relating to freedom of expression and privacy, to avoid confusion over who reports to whom, as well as formalizing processes for monitoring and follow up. This could include systems to share information with other internal company teams who may encounter similar issues and facilitate learning within the company.
- Creating a centralized human rights program within the company to enhance current activity to implement the GNI Principles and ensure that structures are in place to improve implementation during periods of growth or change.
- Integrating commitments to GNI into the hiring and onboarding of staff, such as including human rights as a company value within the hiring process, with considerations for those roles that directly engage with freedom of expression and privacy rights. Consider developing or enhancing onboarding programs for new employees, including those directly responsible for government requests.
- Making processes for escalation of freedom of expression and privacy issues to higher levels of the company sufficiently resilient in the face of increasing interest from employees as well as the public.

Due Diligence and Risk Management

Recommendations to consider under due diligence and risk management, include:

- Periodically reassessing company human rights policies and guidelines. This could include risk assessments and determinations about the most salient or material risks the company faces with regard to freedom of expression and privacy.

- Implementing a process, with dedicated resources, to perform due diligence around business relationships other than suppliers. This could include taking extra steps to address safeguards for freedom of expression and privacy with third-party relationships. Such third-party relationships range from network operator site leases, agents, and partners to Internet company developer communities.
- Enhancing efforts to mitigate freedom of expression and privacy risks from suppliers by mapping out how different functions within the company — security, supply chain, legal — engage with suppliers. This would help determine how to further strengthen oversight of supplier performance.
- Developing and implementing appropriate processes to conduct human rights due diligence and/or impact assessments when divesting.
- Integrating the results of human rights due diligence (HRDD) and HRIAs into overall company risk reporting. This could entail providing guidance on the use of company risk tools and ensuring they are being used for freedom of expression and privacy issues.

Freedom of Expression and Privacy in Practice

Recommendations to consider under freedom of expression and privacy in practice, include:

- Developing country-specific policies and procedures to assist local personnel in operationalizing company-wide policies to implement the GNI Principles, in view of the challenges that arise in implementing the Principles in different countries.
- Considering a centralized system to track implementation of policies and procedures relevant to the GNI Principles across company business units.
- Conducting periodic internal audits of company law enforcement response functions to help ensure the consistent application of policies and procedures.
- Strengthening efforts to seek the assistance, as needed, of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction or demand that appears overly broad, unlawful, or otherwise inconsistent with international human rights laws and standards on freedom of expression or privacy.

Transparency and Engagement

Recommendations to consider under transparency and engagement, include:

- Increasing transparency to users, when permitted by law, about how long government requests, including personal information provided by governments in the request, are retained by the company.
- Promoting curiosity within the company on freedom of expression and privacy, to raise awareness and enhance consideration of these rights in the company's activities.
- Working with multistakeholder coalitions comprising companies, civil society organizations, and others, to engage with governments to encourage legal reforms that would enable the company to disclose to its customers that they have been the subject of a government request, provided such disclosures do not interfere with an ongoing government investigation or national security interests.
- Encouraging more frequent multistakeholder gatherings and work with GNI to facilitate engagement at the local level to better understand the impact of company operations in specific geographic areas.

Recommendation to Companies During the 2015/2016 Assessment Cycle

In the 2015/16 assessments, the assessors presented recommendations to the four previously assessed companies. The recommendations are for the company to consider.[32] Below are some examples of recommendations made to one or more companies being assessed in 2015/2016 as well as some examples to illustrate how they have chosen to act upon them.

EXAMPLES OF RECOMMENDATIONS MADE TO ONE OR MORE COMPANIES IN 2015/2016	EXAMPLES OF FOLLOW UP AND IMPROVEMENTS, NOTED BY THE ASSESSORS, BY ONE OR MORE COMPANIES THAT RECEIVED THIS RECOMMENDATION
Implementation of the GNI Principles in regard to business partners and newly acquired companies.	
When integrating an acquired company into a company's operations, ensure that privacy policies, terms of use, and other relevant policies that are communicated to users are updated and that users are clearly informed which policies are now applicable.	Aligned policies and procedures and brought acquired companies under existing human rights frameworks and teams.
When the operations of an acquired company are not integrated, the acquired company's policies and procedures for handling government requests for user data and content restriction should be reviewed for consistency with the GNI Principles and be updated as necessary.	Established formal due diligence guidelines for mergers and acquisitions to establish when additional human rights due diligence is necessary to ensure consistency with the GNI Principles.
Implementing Human Rights Impact Assessments[33]	
Identify ways to educate and inform employees on the varying scopes of HRIAs in internal company processes to avoid potential for confusion (HRIAs conducted by companies can differ significantly in scope, focus and duration and sometimes are not referred to by this name).	More effective integration of findings from human rights due diligence back into business processes. Evolution of the use of the terms HRDD and HRIA to conform with the broader business and human rights conversation and the GNI Principles and Implementation Guidelines.

32 Process Review Question 6.4 asks the assessor to "Please evaluate whether and how the company has implemented the assessor and board recommendations that were made in the previous assessment process. Please explain whether the company has implemented a recommendation, is in the process of implementing it, or has decided not to implement the recommendation as suggested but has chosen to address the specific issue in another way. Also, as previously noted, Appendix V of the Assessment Toolkit states: "Engagement with recommended steps in a prior assessment shall be considered as an important factor by the board in concluding whether the GNI Company is making good-faith efforts to implement the GNI Principles with improvement over time."

33 The GNI Principles and Implementation Guidelines originally referred only to HRIAs. Updates to these documents published in 2017 fully aligned them with the UNGPs and referred to HRDD as well.

EXAMPLES OF RECOMMENDATIONS MADE TO ONE OR MORE COMPANIES IN 2015/2016	EXAMPLES OF FOLLOW UP AND IMPROVEMENTS, NOTED BY THE ASSESSORS, BY ONE OR MORE COMPANIES THAT RECEIVED THIS RECOMMENDATION
Consider whether to formalize or further formalize HRIA processes undertaken when acquiring new companies that offer services or products that are new to the acquiring company, as well as when selecting new business partners.	Increased use of formal HRIAs, particularly for new technologies.
Improve Communications with users	
Provide more detail to users (with more consistency across different communications channels) on how companies handle requests for their data or government requests to restrict access to content. This includes how government requests for content takedowns are responded to.	Creation of reporting hubs and help centers that house transparency reports and other public documents about responding to government requests for user data and content removal.
Examine options, where relevant, for notifying users of online services when the company will provide a government with data (content or non-content) pursuant to a lawful request, unless notification is prohibited by law.	Unification of policies across different services offered by the same company. Improved notification to users who wish to access or have posted content restricted as a result of government requests.
Provide more information on laws and regulations that impact freedom of expression outside the U.S., by country.	The notification to users when content is blocked within a particular country as a result of a government request includes a link to learn more about legal complaints. Such complaints are also shared with the Lumen project.

Recommendations to GNI to Improve the Assessment Process

GNI, like its members, is committed to improvement over time. This assessment cycle is the culmination of a process of review that began shortly after the completion of the 2015/2016 assessment cycle (see Appendix II). This section first presents assessor recommendations from the previous cycle of assessments and actions taken by GNI in response to them. It then summarizes assessor recommendations to GNI from the current cycle.

Assessor Recommendations to GNI from the 2015/2016 Assessment Cycle

RECOMMENDATION	STEPS TAKEN BY GNI
Clarification and alignment of new Assessment Guidance and Reporting Framework[34] to reduce inconsistencies and align the content of the main themes: Governance, Risk Management, Implementation, Follow up and Improvement, and Transparency.	GNI developed and published the Assessment Toolkit in order to streamline the assessment methodology in a comprehensive one-stop document. • Appendix I of the Assessment Toolkit offers the process review questions organized in the five main themes providing guidance on what to include in each area with reference to the applicable guidelines. • Appendix IV of the Assessment Toolkit maps the GNI Principles to the Implementation Guidelines, providing clarification to assessors.
Further streamline the assessment process to make it more efficient, especially for the assessment of new and smaller-sized companies in the future and to manage the determination of a larger number of assessments.	• Timing of GNI assessment is aligned with member companies' sustainability assessment and reporting cycle. • Use of templates, including Appendix I and II of the Assessment Toolkit, to make reports more consistent. • Suggested word counts in the process review to make reports manageable and comparable. • Assessment review meetings held on a staggered basis throughout the year.
Improving the Case Selection Guidance provided by the GNI non-company members as part of the case selection process and further aligning this document with the assessment methodology.	• Section 3.2 of the Assessment Toolkit further refines the case selection process and criteria, including with respect to the number, types and topics of cases as well as their prioritization. • The Case Selection Guidance document provided by the GNI non-company members includes background information, specific focus topics, and case selection criteria in line with Section 3.2 of the Assessment Toolkit. • Cases proposed by GNI non-company members (civil society, academics, and investor representatives) are aligned with Section 3.2. of the Assessment Toolkit.

[34] The Assessment Guidance and Reporting Framework were the guidance documents used in the previous assessment cycle. These have been replaced with the Assessment Toolkit.

Assessor Recommendations to GNI from the 2018/2019 Assessment Cycle

Improvements to the Process Review: Assessors noted that some questions contained very similar wording and addressed the same or closely related topics for assessment, particularly those concerning a company's engagement with governments. They recommended that the process review questionnaire be reviewed for potential repetitions and redundancies and suggested other adjustments to improve the quality of responses in some sections.

Improvements to the Case Studies: Assessors noted that some of the cases proposed by GNI's non-company constituencies covered several sub-cases, which made it difficult to see the rationale behind the case and to remain within the set word count. They recommended that the non-companies include a rationale for case inclusion, with an explanation as to why a case was suggested; state the objective for the case inclusion; and respond to a number of specific and targeted questions in relation to the case objective identified.

HRIAs: Assessors noted that adjustments to GNI's approach to HRIAs could benefit from additional focus. This could include giving consideration to the sometimes-fluid nature of such assessments, in addition to the articulation of expectations or good practices for the use of HRIAs in specific scenarios (see the Learning and Opportunities Section for more on this topic).

Grievance and Remedy: Assessors suggested that GNI clarify the scope and application of the guideline on grievance mechanisms in light of the specific challenges around the provision of grievance and remedy by ICT companies in the context of government demands and requests.

4) Lessons & Opportunities

4) Lessons and Opportunities

"The GNI multistakeholder model provides a unique platform for civil society, academia, companies, and investors to come together and weigh out their respective priorities toward a consensus. This process is full of critical learning for all stakeholders; something that the world can do with more of! Ultimately, none of the stakeholders have their agenda agreed upon completely, but there is a lot more understanding, empathy, and impact on future course of policy for all."

USAMA KHILJI, Bolo Bhi

The assessment reports, as well as discussions between the GNI Board and each company and its assessors, illustrated important points of progress as well as new and ongoing challenges and opportunities for companies across a variety of operating environments. There is no one-size-fits-all approach to implementing the GNI Principles, and the assessments show how different types of companies adopt policies and practices appropriate to their business models and global presence. They also show that companies' responsibilities for freedom of expression and privacy rights do not exist in a vacuum, but depend upon the actions of external actors, from the governments that determine legal frameworks and make requests and demands, to other actors in industry, as well as civil society, academia, and other experts and affected groups.

This section summarizes key lessons from across all 11 company assessments from which good practices may be developed and identified and which may benefit from a collaborative approach. GNI and its membership will consider ways to integrate these issues into its private and public learning agenda, developing tools and guidance to improve knowledge sharing and our overall framework.

Internal Challenges and Opportunities

Integrating Freedom of Expression and Privacy into Business Operations

The GNI Principles and Implementation Guidelines provide a flexible approach to integrating freedom of expression and privacy into company operations. The assessments illustrate the different approaches taken by companies, with varying advantages and constraints. For example, companies may choose to centralize GNI functions within a dedicated human rights team, which empowers highly trained internal champions within the company. This is considered good practice, and when companies take this approach, they should ensure attention is paid to integrating human rights awareness and responsibilities

across the entire company's culture. Companies also may learn from each other about how to manage geographical as well as functional teams, to ensure that frontline teams based in different parts of the world can learn from each other, with appropriate support from headquarters. The different types of companies participating in GNI — Internet companies, telecommunications network operators, and equipment vendors — face distinct challenges which will also have an impact on how they structure their implementation of the GNI Principles. Future GNI learning activities may further consider the tradeoffs that arise from different operating structures and opportunities for improvement and consider how GNI can address freedom of expression and privacy rights across the full ICT value chain.

Escalation

Ensuring that frontline staff who receive government requests and demands are able to efficiently and effectively escalate appropriate requests to senior management is a key component of the GNI Principles. The GNI Board noted several instances of good company practice in this area across the assessments. For example, one company had a system whereby headquarters staff are on call to deal with serious requests. Another practice that can complement such procedures is the provision of granular guidance for local staff on how to implement company policies in response to local laws.

Training

A key challenge identified during these assessments is how to effectively train appropriate parts of often vast, growing, and globally distributed company workforces. The majority of assessments noted training as an area where improvements could be made to company implementation. In particular, several assessments recommended enhancements to the monitoring and evaluation of training initiatives to be able to better evaluate their efficacy. Another potential good practice is to combine top-down and bottom-up approaches to training, to generate awareness and a broader culture of human rights within a company. A possible topic for future learning within GNI is whether the development of GNI-specific training materials, or the integration of material developed collaboratively through GNI into existing trainings, could add value to existing company training programs.

HRDD and HRIA

The relationship between human rights due diligence (HRDD) and human rights impact assessments (HRIAs) is an area of focus not just within GNI but across the wider ecosystem of business and human rights. However, the way in which these two sets of complementary processes function and interact can be distinct in the context of the ICT sector. Given the dynamic nature of the ICT sector — both in terms of the underlying technologies and uses, as well as the regulatory environment — HRDD and HRIAs must be designed to account for constant change. The assessments show that companies are evolving their approaches by integrating impact assessment into wider due diligence systems, which vary from company to company, and even within companies, with regard to products, markets, and other topics and types of risks. Several assessments noted the importance of standalone HRIAs at varying levels, from global company HRIAs to those focused on specific countries, issues, or business decisions. Relatedly, some assessments illustrated the importance of having procedures that are fit-for-purpose and designed for rapid and efficient deployment. Other areas for future learning within GNI include the identification of good practices for HRDD on research and development and product design, as well as collective work by GNI members to inform HRDD on emerging issues.

User Notification

The GNI Board noted that the practice of providing notification to users when their data is requested by governments varies depending on the legal frameworks under which companies operate.

External Challenges and Opportunities

Multistakeholder Engagement

Several cases, including the Paraguay case summarized in this report, showcase the role of companies in engaging with multistakeholder coalitions to support freedom of expression and privacy rights and to jointly advocate with governments on specific laws and regulations. Such efforts can and should vary depending on the local context, but there is an opportunity within GNI to develop good practices to improve collaboration between companies and local civil society and other key stakeholders. Possible elements of good practice could include the formation of advisory networks and developing criteria for when an issue could warrant outreach to higher level external experts (such as relevant national, regional, or global human rights institutions). In addition, considerations around how companies may engage with actors who may often have opposing viewpoints but could be aligned on a particular issue should be further explored. Looking ahead, GNI will collaborate with its membership in different parts of the globe to explore opportunities to support multistakeholder coalitions at the national or regional level.

Ongoing Challenges Around State Surveillance, Including Direct Access Regimes

Legal prohibitions on the disclosure of information related to national security requests and concerns for safety of local personnel continue to be a legitimate obstacle to companies' ability to be transparent about these requests. The assessments, including several case studies, addressed steps companies have taken to increase transparency notwithstanding these challenges. These include enhancements to company transparency reporting, challenging gag orders in court, and advocating against laws that would make it more difficult for companies to be transparent. A particularly challenging issue is direct access regimes, where national laws require companies to facilitate unmediated technical access by authorities to company networks, so that government actors can obtain user data without having to make individualized requests to the companies. Many of these laws and their implementing regulations and/or orders are confidential, posing particular challenges with regard to transparency and user notification. In more permissive operating environments, companies and other stakeholders may have greater opportunities to advocate against such practices and provide some degree of transparency around them. In more restrictive environments, room for maneuver is limited.

Network Disruption Orders

Instances of government-ordered network disruptions increased during the assessment period. Six case studies covering seven countries around the world examined specific instances of network disruptions and service restrictions. These case studies showed that national legal frameworks and license obligations fail to provide appropriate levels of legal clarity and restrict the ability of network operators to challenge government demands for network disruptions. In many cases, the requests that operators receive provide reference to the law the government asserts that authorizes the disruption, but do not include judicial authorization, set out the government's legal theory, or explain the rationale for the requests. Instead, the orders simply state the location and duration of the required disruption, at times also stipulating the projected penalties for non-compliance. In addition, the cases showed that credible security risks to company personnel often necessitated compliance with requests. Despite these constraints, the case studies did show that companies were able to mitigate some negative impacts of network disruptions:

Documentation and Escalation: In some cases, network disruptions were primarily conveyed via verbal requests. By engaging in dialogue with government authorities, several

companies succeeded in securing written orders from governments that are signed, dated, and state the specific legal provisions that authorize them. Company requirements that such requests be escalated to senior management at the headquarters level contributed to securing such written orders. These measures also help prevent situations where local companies accede to a disruption order without the awareness of headquarters.

Narrow Interpretation and Application: Although protection of employee safety may require compliance with overbroad disruption orders, companies may nonetheless be able to engage with authorities or identify other means of achieving a narrow interpretation of a disruption order that could minimize the negative impact. For example, an order might specify specific websites or services rather than mandating wholesale disruptions. Companies can engage with authorities to clarify the specific geographic scope of an order and implement the order as specifically as feasible to limit its geographic impact. Or technical measures might be able to exempt key infrastructure, such as hospitals, from a disruption.

Transparency: Companies may be limited in their ability to notify users about a disruption. In some cases, companies have taken advantage of the lack of any affirmative prohibition to notify users, or resisted government requests to issue public statements that provide a false reason for a government-ordered disruption, such as a technical problem.

Content Challenges

Multiple cases examined as part of this assessment cycle explored the increasingly complex issues at play in government requests for content removal. The previous assessment cycle identified "extremist" or "terrorist" content as a key challenge, and it continues to present new difficulties for companies, as law enforcement and security agencies push for faster removals. The cases show that companies have robust and mature systems to direct governments to follow their own legal procedures as well as company policies, to better enable them to scrutinize and respond appropriately to such demands.

New issues have risen to the forefront of global content concerns, including the live streaming, targeting, and amplification of "abhorrent" acts, as well as other issues that pose content challenges, from hate speech to disinformation. In addition to the increasing number of reasons why content should be removed, companies are also dealing with government requests requesting removal of new and complicated types of content. Although URLs, websites, and search results continue to be subjects of removal requests, companies are also receiving requests to block or restrict access to applications and services, particularly messaging applications. In several cases, such requests were for companies to remove these services from digital distribution services or app stores. The cases illustrate that the same policies and procedures that companies have been using to implement the GNI Principles are also applied in these instances.

5) Looking Ahead

5) Looking Ahead

This cycle of assessments shows the different ways that a growing number of companies from across the ICT sector are exercising their responsibility to respect the freedom of expression and privacy rights of users and customers in different jurisdictions around the world. They also show the increasingly sophisticated measures that governments are employing to assert control over online content and digital communications.

The 86 case studies reviewed by the GNI Board make clear the stark challenges for freedom of expression and privacy rights now and in the near future. Whether it is governments who are genuinely committed to human rights but facing vexing challenges around disinformation, cybercrime, hate crimes, or terrorism, or governments who are actively seeking to suppress their citizens' rights, the operating environment for rights-respecting ICT companies is getting more complex.

No single company or constituency can turn this tide on their own. Creating an enabling environment for freedom of expression and privacy rights will require the efforts of governments, companies, and other key actors including investors, academics, and civil society organizations inside and outside GNI.

First, states committed to human rights must lead by example to craft clear laws and regulations to confront contemporary ICT sector challenges while protecting freedom of expression and privacy. Democratic, rule-of-law abiding states can demonstrate good practice both by implementing transparent, multistakeholder consultative, empirically informed processes to develop new laws and regulations, and by finding clear, creative means to address legitimate challenges with narrowly tailored, appropriate, and accountable measures. GNI urges the members of the Freedom Online Coalition to recall their commitment as part of the 2014 Tallinn Agenda for Freedom Online to "Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same."

Second, companies across the ICT sector should embrace their responsibilities under the UN Guiding Principles on Business and Human Rights and use the GNI Principles and Implementation Guidelines to integrate freedom of expression and privacy rights into their operations. The experiences and insights presented in this report offer guidance to companies on how to apply these standards in a flexible manner across different segments of the ICT sector, from Internet platforms to telecommunications operators and equipment vendors. GNI will continue to reach out to companies across the industry and around the globe to share more about the forum it offers. Moreover, the challenges GNI seeks to address are not limited to tech and telecommunications companies, as a wider range of industries employ ICT innovations and collect personal data of interest to governments. GNI encourages companies in industries ranging from automotive to finance to explore and consider committing to implement the GNI Principles. GNI welcomes interest from these companies and should be considered a

resource for those interested in developing their strategies for operating in a manner consistent with freedom of expression and privacy rights.

"Trust is core from the user perspective. Transparency and accountability help ensure that government access to data is more consistent with human rights principles. The GNI assessment, a multistakeholder process, provides a robust model also for companies outside the ICT sector now increasingly receiving government requests for user data."

PATRIK HISELIUS, Telia Company

Third, companies and states should not address these threats and challenges on their own. In fact, when governments confront companies behind closed doors, risks to freedom of expression and privacy increase. The involvement of investors, academics, and civil society organizations brings much-needed transparency, expertise, and legitimacy to decision-making about the dilemmas in the ICT sector. This does not mean that all stakeholders need to agree about everything. GNI shows that human rights organizations and companies that take starkly different positions on various issues can nonetheless advance principles of freedom of expression and privacy. The assessments this report describes have helped contribute to the trust between participants that undergirds GNI's wider efforts.

It is imperative that all actors work to put the users of ICT products and services, and the protection of their freedom of expression and privacy rights, at the forefront of their efforts to develop, deploy, and regulate new technologies. It is also vital that users themselves demand such protection from governments and companies. At the same time, users and those who advocate for them must continue to protect themselves from violations of their rights.

"The active participation of civil society organizations is crucial in assessing whether companies are living up to their commitment to the principles of freedom of expression and privacy online that lie at the heart of the Global Network Initiative. The process of assessing independently whether companies are making 'good-faith efforts over time' to implement the principles is a work in progress. We realize that it can sometimes be perceived as 'a black box' by external stakeholders. But GNI's assessment process is evolving in the right direction thanks to the hard work and commitment of civil society and the companies themselves, and the trust that GNI has promoted over the last 10 years."

ROBERT MAHONEY, Committee to Protect Journalists

Next Steps

Looking ahead, GNI will work to integrate insights from this assessment cycle into our wider efforts to protect and promote freedom of expression and privacy in the ICT sector. Assessments build trust within GNI's membership that supports shared learning and collaborative policy engagement. After the publication of this report, the following activities will provide additional opportunities for transparency, accountability, and multistakeholder collaboration.

Company Reporting: Within six months of the publication of this report, each of the 11 companies included in this assessment cycle will communicate to the public about the outcome of their assessment.

GNI Review: Consistent with our efforts to enhance the assessment process, GNI will conduct the third review of the process.[35] In order to strengthen our standards and practices, this review will draw from the assessor recommendations to GNI and the insights of its company and non-company members in response to the cases evaluated and the lessons learned from the process review of each company. The review will allow GNI to scale its learning of best practices and develop internal and external-facing policy advocacy and stakeholder outreach.

Shared Learning: GNI will implement a process together with its membership to integrate key insights from the assessments into its learning agenda. This will include confidential learning opportunities for members, as well as public activities including the Annual Learning Forum and the development of tools and guidance for companies on issues such as human rights due diligence.

Public Policy: Insights from assessment will inform GNI's policy priorities and activities on network disruptions, surveillance, intermediary liability and content regulation, and jurisdictional assertions and limits.

[35] Following the first assessment cycle, GNI undertook a review of the process as part of its broader 2014 Strategic Review. Later in 2016 GNI completed a similar exercise after the second assessment cycle.

Appendix I: Acronyms and Abbreviations

AI	artificial intelligence
AOL	America Online, Inc.
APAC	Asia Pacific region
BHRP	Business and Human Rights Program
BSR	Business for Social Responsibility
CELA	Corporate and Legal Affairs
CEO	chief executive officer
CNIL	Commission nationale de l'informatique et des libertés (National Commission of Computing and Freedoms)
CDRs	Call Detail Records
DPIA	Data Protection Impact Assessment
ECJ	European Court of Justice
EK	Confederation of Finnish Industries
EMEA	Europe, Middle East and Africa region
ESG	environmental, social, and governance
ETNO	European Telecommunications Network Operators
EU	European Union
FAQ	frequently asked questions
5G	fifth generation of cellular communications
FiCom	Finnish Federation for Communications and Teleinformatics
4G	fourth generation of cellular communications
FY	fiscal year
GDPR	General Data Protection Regulation
GSMA or GSM Association	Global System for Mobile Communications Association
GNI	Global Network Initiative
GREC	Governance, Risk, Ethics, and Compliance
GRI	Global Reporting Initiative
HMD	Hello Mobile Devices
HRDD	Human Rights Due Diligence
HRIA	Human Rights Impact Assessment
IHRB	Institute for Human Rights and Business
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
ICESCR	International Covenant on Economic, Social and Cultural Rights
IoT	Internet of things
IP	Internet Protocol
ISIS	Islamic State of Iraq and Syria
ISP	Internet service provider
LED	Law Enforcement Disclosure
LEA-MEP	Law Enforcement Response and Major Events Policy
LGBT	lesbian, gay, bisexual, and transgender
LI	Lawful Intercept
LLP	Limited Liability Partnership
NetzDG	Netzwerkdurchsetzungsgesetz (Germany's Network Enforcement Act)
NGO	non-governmental organization
NYSE	New York Stock Exchange
OECD	Organization for Economic Co-operation and Development
1MDB	1Malaysia Development Berhad
Q&A	questions and answers
RDR	Ranking Digital Rights
RFP	request for proposal
SL	sociedad limitada (limited society)
SPOC	single point of contact
3GPP	3rd Generation Partnership Project
TML	Telenor Myanmar
TP	Telenor Pakistan
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNGPs	United Nations Guiding Principles on Business and Human Rights
U.S.	United States
URL	universal resource locator
VOIP	voice over Internet protocol
VR	virtual reality

Appendix II: Assessment Review Recommendations and Responses

In 2016, The GNI Board appointed independent consultant and former GNI Board member Michael Samway to conduct a comprehensive review of issues raised during the second cycle of assessments. After consulting extensively with the assessors and across our membership, Professor Samway presented recommendations designed to enhance the efficiency of the assessment process, and to ensure resources are targeted at producing the most meaningful evaluations. All but one of the recommendations were adopted by the GNI Board, who took a number of decisions to improve the assessment process in preparation for the 2018/2019 cycle. Examples of actions taken in response to these recommendations include the following:

EXAMPLES OF RECOMMENDATIONS	STEPS TAKEN BY GNI
Increase the pool of accredited assessors and revise the assessor training to focus on the scope and methodology of the assessment.	GNI extended its pool of five assessors to a total of 12 through the accreditation process, which verifies that individuals and organizations conducting assessments comply with the independence and competency criteria to carry out this work. In September 2018, GNI delivered a training to all the accredited assessors. The training included an introduction to the Assessment Toolkit, a review of the GNI Principles and Implementation Guidelines, and a discussion about how GNI's assessment process relates to the assurance of sustainability reporting of some companies. The training also covered issues around assessor access to information and limitations on disclosure, including attorney-client privilege.
Increase transparency through publishing additional documentation and information on the GNI website: • Publish updated assessment documentation • Publish thorough Q&A on the assessment process	The Company Assessments page on the GNI website has all relevant information about current and past assessments and the Assessment Q&A offers useful explanations to key aspects of the assessment.
Enhance existing efforts to systematically capture and collect learning points across each assessment.	GNI continues to distill lessons and identify best practices and topics for its learning and policy advocacy agendas throughout the assessment process. Non-company members formed study groups for each company to identify themes to discuss during the board review meetings. A process of reporting to the board on the learning points from the assessments has been developed to build upon previous learning efforts. As part of this process, GNI will explore opportunities to use insights from assessment to inform its wider learning among members and with the public on issues such as HRDD and HRIAs.

EXAMPLES OF RECOMMENDATIONS	STEPS TAKEN BY GNI
Clarify the role of recommendations in the board determination of whether a company is making good-faith efforts to implement the GNI Principles with improvement over time.	The board decided that companies must consider all assessor and board recommendations and may reject, modify or accept and begin to implement recommendations.[36] If the company modifies or rejects a recommendation, it will provide an explanation to the GNI Board. Board recommendations are approved by the (majority vote of the) board, including company board members. Recommendations from individual board members are informal feedback, and not board recommendations. Engagement with recommended steps in a prior assessment shall be considered as an important factor by the board in concluding whether the GNI member company is making good-faith efforts to implement the GNI Principles with improvement over time.

[36] For the avoidance of doubt, GNI is mindful of the antitrust/competition laws. GNI does not dictate the business decisions that its members must take or encourage its members to reach any agreements with respect to a member's business terms, customers, territories, or other competitively sensitive issues.