GLOBAL NETWORK INITIATIVE

The GNI Principles at Work

PUBLIC REPORT ON THE FOURTH CYCLE OF INDEPENDENT ASSESSMENTS OF GNI COMPANY MEMBERS 2021/2022

Table of Contents

1.
Introduction

1. Introduction

GNI was launched in 2008 with the mission of protecting and advancing freedom of expression and privacy rights in the information and communications technology (ICT) sector through multistakeholder efforts to set a global standard for responsible company decision making in the face of government restrictions and demands. In the fifteen years that have followed, GNI has grown to include 90 members across 38 countries in its four constituency groups: academics and academic institutions, civil society organizations, information and communication technology (ICT) companies, and investors. GNI's company membership has diversified to include internet platforms, telecommunications operators, equipment vendors, and other entities providing important services across the ICT sector. All members across all stakeholder groups agree to GNI's **core commitments**, including the **GNI Principles on Freedom of Expression and Privacy** ("the GNI Principles") and the more detailed **Implementation Guidelines** ("the Guidelines"), which are both informed by the **UN Guiding Principles on Business and Human Rights**.

Central to GNI's work is the conduct of periodic, independent assessments of company members' efforts to implement the GNI Principles and Guidelines. This Public Assessment Report (Report) provides an overview of and information about the fourth cycle of GNI assessments, during which eleven GNI companies - BT, Ericsson, Google, Meta, Microsoft, Nokia, Orange, Telenor, Telia Company, Vodafone, and Verizon Media/Yahoo[1] - were assessed for policies that existed and case studies that took place between October of 2019 and October of 2021.

The activities that constituted the fourth assessment cycle were conducted across 2021 and 2022. They coincided with and were shaped by a number of globally-impactful developments. The most obvious was the Covid pandemic, which was declared a Public Health Emergency of International Concern just two months after the preceding, third cycle of GNI assessments was completed. Thanks to the creativity and persistence of our members, assessors, and staff, much of the preparatory assessment-related work was successfully conducted remotely. However, the indirect impacts of the pandemic on the workflows, resources, capabilities, and focus of all involved were innumerable. A number of case studies and recommendations shared in this Report provide insight into the ways in which Covid impacted the use of ICT products and services, the types of demands that governments made of companies, and the dynamics between companies, governments, and other stakeholders (a case study supplement will be published separately and **appended** to this report).

> The amount of work that the assessors, the Board, company members, and the staff put into the assessment process is really impressive, and is reflected in the incredible breadth and depth of issues that are addressed.
>
> JASON PIELEMEIER, GNI Executive Director

Fortunately, conditions had improved significantly by the time the Board's Assessment Review Meetings (ARMs) began in early 2022, allowing for three out of five ARMs (covering 7 of the 11 companies) to be conducted in a hybrid manner. Covid also underscored the resilience, reliability, and capabilities of today's global ICT networks,

1 In 2021 Verizon sold Verizon Media (now known as Yahoo) to funds managed by affiliates of Apollo Global Management. Yahoo now operates as a standalone company under Apollo Funds. The sale of Yahoo took place at the end of this assessment cycle.

while simultaneously exposing accessibility gaps, differences in legal frameworks, and inconsistencies in business conduct across the sector - all of which had implications for and were reflected in the assessment reports.

The assessment cycle also corresponded with an uptick in civil and interstate armed conflict, with particularly significant episodes of violence occurring in Afghanistan, Myanmar, Syria, and Ukraine. The full-scale Russian invasion of Ukraine occurred just after this assessment period and only three-months prior to the first ARM, which took place in Stockholm in May 2022, just as the Finnish and Swedish governments officially decided to apply for NATO membership. The impacts of these conflicts on GNI's members and their implications for our work echoed throughout the assessment reports and discussions, and have continued to shape the work of GNI, including motivating the establishment of an Armed Conflict Working Group under GNI's Policy Committee, in 2022.

The fourth assessment cycle also took place during a period of intense regulatory activity that had direct and indirect impacts on the assessment exercise. While GNI assessments have always helped illustrate the ways governments misuse legal authorities to limit freedom of expression and privacy, during this cycle we began to examine the implications of government efforts to affirmatively support human rights and responsible business conduct through regulation. The most significant legislative development for the ICT sector during this period was the European Union's Digital Services Act (DSA), which was introduced in December 2020 and approved in October 2022.

Over the same period, a number of relevant jurisdictions advanced legislation mandating human rights due diligence (mHRDD). The assessment of Orange, which became subject to the French Duty of Vigilance Law (*Loi de Vigilance*) prior to this cycle, was the first but will certainly not be the last one to examine how implementation of the GNI Principles can prepare a company for compliance with mHRDD, and how such laws can support the implementation of the GNI Principles.

The GNI assessment is the longest-running, most comprehensive mechanism for sharing non-public information across stakeholder groups about the commitments and methods that ICT companies have undertaken to protect freedom of expression and privacy. We invite readers to read this report carefully in order to understand how users, civil society, and government actors benefit from these efforts, and to learn how you can engage with GNI to support them.

KEY NUMBERS OF THE FOURTH ASSESSMENT CYCLE

2 EQUIPMENT VENDORS

5 TELECOS

4 INTERNET COMPANIES

*including 2 first-time companies assessed

6 ASSESSORS SELECTED TO PERFORM ASSESSMENTS

114 INTERVIEWS

88 CASE STUDIES

68 CASE STUDIES RESPONDED TO SUGGESTIONS BY GNI NON-COMPANY MEMBERS
civil society organizations, investors, and academics

22 BOARD MEMBERS

10 COMPANY BOARD MEMBERS

12 NON- COMPANY BOARD MEMBERS

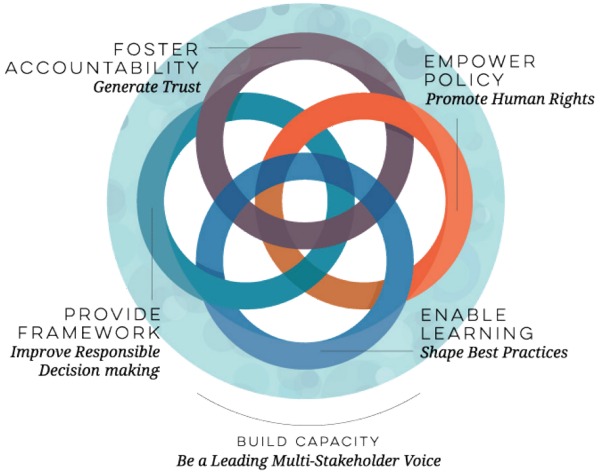
2. Executive Summary

2. Executive Summary

The four pillars on which GNI's work is built – providing a *framework*, enabling *learning*, empowering *policy*, and fostering *accountability* – inform each other on a perpetual basis as technology and its uses evolve over time. GNI's unique assessment process is the primary mechanism through which GNI fosters accountability. This Report provides insight into the assessment process, shares lessons and learnings drawn from the assessments, and informs the public about the ways in which GNI companies and GNI as an organization are working to foster responsible company decision making to advance freedom of expression and privacy around the world. It supplements other information that GNI companies have made public consistent with the commitments to transparency set out in the GNI Principles and Implementation Guidelines.

GNI's fourth assessment cycle, conducted during 2021 and 2022 and covering company policies and cases during the period between October 1, 2019 - October 1, 2021, evaluated the efforts of 11 GNI member companies, including telecommunications operators, equipment vendors, and internet companies. Of these companies, nine underwent at least their second complete assessment cycle. In order to compile their reports, assessors received access to information, including relevant documents, in secure settings and connected with key company personnel from frontline teams to senior management, conducting a total of 114 interviews. In total, this assessment cycle included the examination of 88 cases in a variety of operating environments, including specific responses to government demands, as well as cases regarding the broader context of company operations.

Following a **detailed description** of the assessment process, this report provides **summaries of the independent assessments** of all 11 companies, including the GNI Board determination, the assessors' findings, the Board's discussions, and recommendations. While we have endeavored to include as much information as possible, there is a well-recognized tension between disclosure and the need to protect the ability of GNI members to continue pushing back on



overbroad and inappropriate government demands and restrictions. Where possible, we have attributed recommendations and case studies. In other situations, we have anonymized or aggregated them to provide key learning points without compromising security and confidentiality.

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. It draws trends from the wealth of information shared and discussed throughout this assessment cycle to identify the **range of challenges** that GNI and its members face as governments become more innovative and assertive in their approach to technology, as well as opportunities for continued creative and collaborative efforts to enhance freedom of expression and privacy around the world. Finally, the report **concludes with a reflection** on the ways GNI will continue to evolve, including through changes to our assessment process, to maximize our impact going forward.

3.

About the Assessment

3. About the Assessment

During each assessment cycle, independent assessors accredited and trained by GNI are provided an internal look at GNI member companies' processes, policies, and procedures that relate to freedom of expression and privacy. In addition to verifying and reviewing these processes, assessors and assessed companies explore their use and effectiveness in practice via the examination of a select group of case studies. Each assessor produces a confidential assessment report consisting of distinct Process Review and Case Study portions, as set out in the GNI Assessment Toolkit ("the Toolkit" or "Assessment Toolkit"). These reports describe how the company is working to implement the GNI Principles and Guidelines and identifies ways in which those efforts can be strengthened. These reports are shared with GNI's Board in advance of that company's Assessment Review Meeting ("ARM"). At the ARMs, Board members ask detailed, clarifying, substantive, and contextual questions about the assessment report before voting on a final determination as to whether the company is making good-faith efforts to implement the GNI Principles with improvement over time.

THE ASSESSMENT TOOLKIT

GNI's Assessment Toolkit is a comprehensive instructional document for the entire assessment process. It provides a robust structure for conducting both the process review and case study portions of the assessment, and is publicly available on the GNI website. In addition to being used to conduct independent assessment, companies use the Toolkit to conduct a self-assessment after their first year of GNI membership, before they are independently assessed by GNI assessors at the next assessment cycle. The Toolkit is also intended to be a public resource that any company can use to understand and consider ways to structure relevant internal systems and processes.

KEY TERMS

"A GOOD FAITH EFFORT TO IMPLEMENT THE GNI PRINCIPLES WITH IMPROVEMENT OVER TIME"

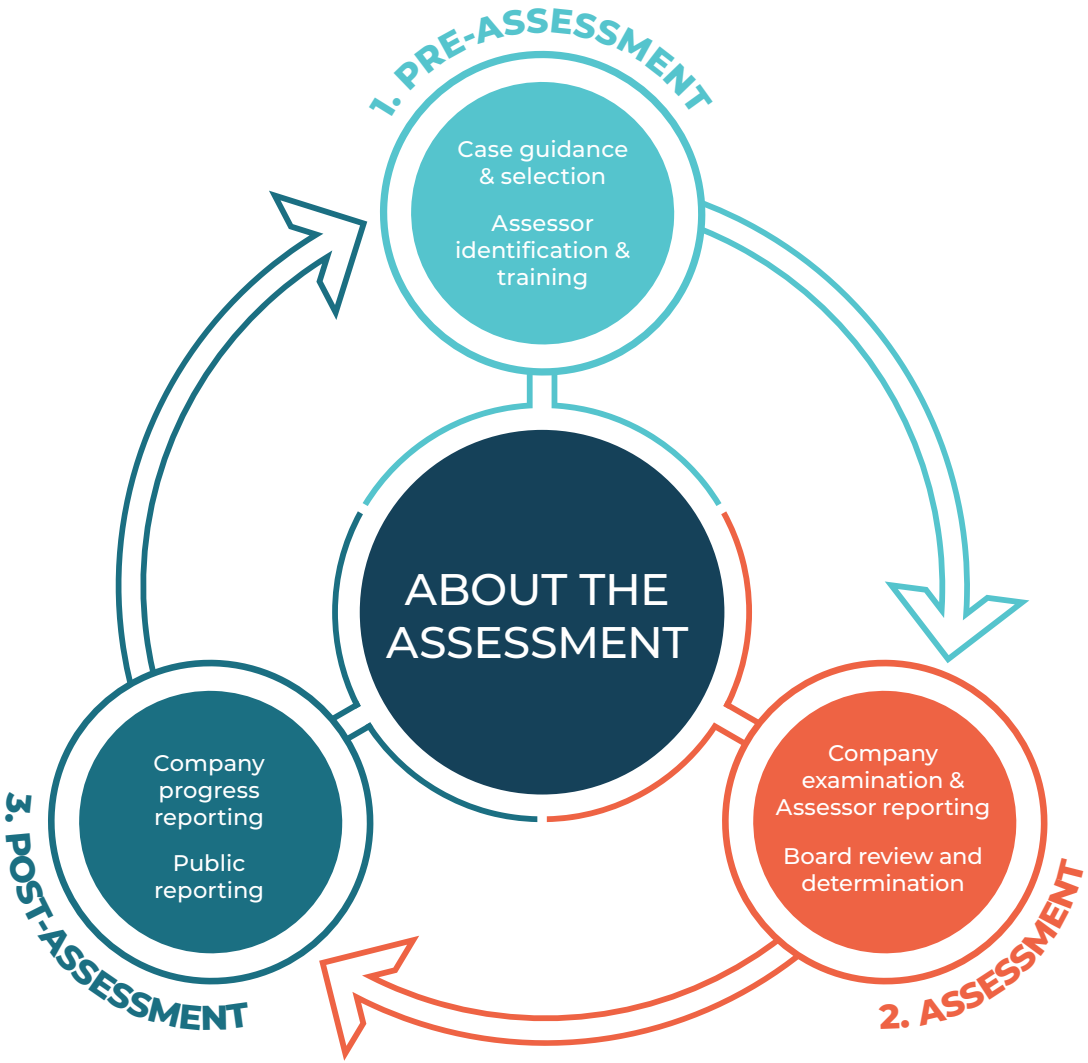
Rather than ascribing a definitive but fleeting rating to a company's efforts, GNI's threshold of a good faith effort with improvement over time reflects the evolving technological ecosystem in which new developments present new risks and shifting legal frameworks perpetually change company-government interactions and pressures.

PROCESS REVIEW

The **Process Review** is the portion of the assessment intended to ensure that companies have systems, policies, and procedures in place to implement the GNI Principles. It consists of specific short answer, long answer, and yes/no questions about the company's policies, personnel, and practices.

CASE STUDY

The **Case Study** portion is the examination of specific instances to demonstrate whether and how a company's systems, policies, and procedures were implemented in practice, particularly when responding to government requests and demands. Case studies are not meant to be statistically representative, and the assessment does not judge how a company handled any individual case. Instead, the cases are intended to provide assessors and Board members with a more specific understanding of how systems, policies, and processes are used in order to review whether and how companies are implementing the GNI Principles in practice.



1. PRE ASSESSMENT

Assessors trained and accredited by GNI, and contracted with the assessed company, work alongside GNI's non-company constituency and the company to identify appropriate cases for assessment.

2. ASSESSMENT

The assessors examine company documents and conduct interviews to answer the questions presented in the Assessment Toolkit's **process review,** as well as present **case studies** that exemplify those processes. Completed reports are subject to thorough scrutiny by GNI's non-company board members ahead of an open conversation involving the GNI Board, the company, and the assessor about the contents of the report. The GNI board then votes confidentially to determine whether the company is making ***a good faith effort to implement the GNI Principles with improvement over time***.

3. POST-ASSESSMENT

Both GNI and its assessed companies are obligated by the GNI Policy, Accountability, and Learning Framework ("The Framework") to report publicly on the results of the recent assessment cycle. Additionally, companies must follow up on any recommendations issued during the assessment meeting within one year of the assessment and address previous recommendations in future assessments.

1. PRE ASSESSMENT

ASSESSOR IDENTIFICATION AND TRAINING

Accredited assessors are organizations with expertise in legal & human rights standards and compliance & auditing and who meet GNI's **Independence and Competency Criteria**. Potential assessors must submit individual CVs to the GNI staff for consideration, and it is expected that those leading the majority of the assessment work on behalf of the assessor will be individuals whose CVs have been submitted during the accreditation process. Selected assessors must attend a training session organized by GNI prior to conducting an assessment, and accredited assessors enter a master services agreement (MSA) with GNI as detailed in the **Governance Charter** in order to complete the accreditation process. A **complete list of GNI's accredited assessors** can be found on our website.

A company may select any assessor from the pool of accredited assessors to conduct its assessment, at which point the two entities will enter into their own agreements detailing such matters as the cost of and timeline for the specific assessment.

> GNI's assessment process has evolved over time to address new technological developments, the growing diversity of products and services offered by GNI's company members, and changes in how government make demands of technology companies that are inconsistent with international human rights law. The flexibility of the core GNI Principles in the face of these changes makes the framework it provides for assessment dynamic, yet enduring.
>
> **VIVEK KRISNAMURTHY, Assistant Professor at the University of Colorado Law School**

The nature of the assessment requires assessors to access some of the company's non-public information. Assessors are subject to confidentiality duties in accordance with antitrust law and other requirements that may bar companies from disclosing certain information.[2] Further, the content of each assessment report remains confidential even after the board determination is made, including in this Report, unless and until the Board agrees for it to be made public.

Confidentiality is a pivotal element of the process; it affords stakeholders the opportunity to have a freer, more open conversation that is useful both to companies seeking advice and to the non-company members seeking to understand the internal human rights processes of company members. Noting that such confidentiality has the potential to interfere with information relevant to the assessment, assessors are required to state in each report whether they had been given sufficient information to conduct the assessment, and are encouraged to raise any concerns about their access to information with the GNI Executive Director throughout the process.

CASE GUIDANCE AND SELECTION

GNI's multi-step, multi-stakeholder case selection process begins with a **case selection guidance template** compiled by GNI's non-company members outlining the information required and appropriate format for identifying potential case studies. Next, GNI non-company members (through the Case Selection Guidance Working Group - CSGWG), the company being assessed, and the assessor each use their own expertise to identify possible cases for consideration. The ultimate case study list is agreed upon by the company and assessor – however, if any cases recommended by the CSGWG are not selected for review, the final assessment report must explain the reasoning for their exclusion.

Case studies must meet the criteria detailed in section 3.1 of the Assessment Toolkit. The recommended distribution of cases is four (4) exploring specific government requests/demands; two (2) regarding freedom of expression; two (2) regarding privacy concerns; and a strong recommendation for including two (2) cases concerning due diligence processes. Typically, eight (8) cases are

2 For more detail on limits, see section 4: 2021-2022 Assessments

included in the final assessment, although departure from this format may be justified depending on the size, complexity, or nature of the company (e.g. equipment vendors do not typically receive content removal demands from governments) or in recognition that a single case may cover multiple topics.

2. ASSESSMENT

COMPANY EXAMINATION & ASSESSOR REPORTING

Once cases are finalized, assessors spend up to six months examining internal company documents and communications as well as conducting interviews with relevant company personnel in order to compile an assessment report. The Assessor will consult with the Executive Director and Independent Chair of GNI at or about the midpoint of this process to update them on the status of the assessment, request guidance, and/or raise concerns about the assessment. The company being assessed is welcome to participate in this consultation.

The assessment report is initially drafted by the assessor and/or company, and must follow the format outlined in Appendices I and II of the Assessment Toolkit. For any pieces of the report drafted by the company, the assessor has a duty to verify the facts outlined therein. The report is then reviewed and revised by the assessor, and the company is given a reasonable opportunity to identify factual errors, suggested revisions, and confidential information for exclusion. The assessor prepares the final draft of the report, which includes recommendations on ways the company may be able to make further improvements related to its implementation of the Principles and Guidelines, and provides the company with one last opportunity to review it before it is securely transmitted to the GNI board, at least two weeks ahead of the Assessment Review Meeting.

BOARD REVIEW & DETERMINATION

Upon receipt of the assessment reports, GNI's non-company board members divide into groups and split the responsibility of thoroughly reviewing each report and identifying questions for the company and assessor to address at the company's ARM. To ensure an open discussion, the Board agrees ahead of time on expectations for how the ARM will be conducted. Each ARM comprises a statement by the assessor, a discussion between the assessed company and the GNI board, and a determination vote.

> The assessment process is a useful and valuable way of increasing the transparency of how companies analyse human rights issues and handle risk management. As an assessor, it is an important to be able to communicate and understand the nuances of how companies handle these issues and risks, and we find that the Assessment Toolkit provides an effective approach for assessing company progress in this area.
>
> MARK TAYLOR, Osborne Clark

The assessor begins by addressing whether they had access to sufficient information and expanding on any challenges they encountered. During this segment, Board members ask the assessors both substantive and procedural questions about the process and assessors share the recommendations they recorded for the company and for GNI. The assessor departs the room, and the Board engages in conversation with the company about the content of the assessment, again asking substantive and procedural questions. Companies being assessed shall be prepared to provide contextual information to inform the discussion, excluding information admitted for confidentiality reasons.

Finally, representatives of the company being assessed exit the room while a confidential vote is held to determine whether the company is making a good faith effort to implement the GNI Principles with improvement over time, and to discuss any formal recommendations they would like to make to the company in addition to those provided by the assessor. Company representatives are then invited back into the room to be notified of the board's determination and any formal Board recommendations.

3. POST-ASSESSMENT

PUBLIC REPORTING

After an assessment cycle is completed, GNI reports publicly on the outcome of the process as outlined in GNI's Accountability, Policy, and Learning Framework (Appx. III of the **Assessment Toolkit**). GNI's Public Assessment Report – this document – must include a summary of the progress made by GNI and its member companies; a statement on collective lessons learned regarding the Principles and Implementation Guidelines; information to improve the understanding of threats to freedom of expression and privacy across various sectors, geographies, and legal and cultural systems; and the board's determination of compliance or non-compliance for each assessed company.

Under the framework, companies are also required to publicly report on the results of their GNI assessment within six months, in a manner of their own choosing.

COMPANY PROGRESS REPORTING

Within a year of the assessment's conclusion, companies are to report back to the GNI Board on the steps they have taken to implement recommendations received through assessment.

4.

2021/2022 Assessments

4. 2021/2022 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.[3] 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, written responses to specific questions, access to secure documents on the screens of company personnel, and examining documentation of incoming government requests and outgoing company responses.

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. 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.

3 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."

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 on implementing the GNI Principles during the assessment period as it makes this determination.[4]

ASSESSED COMPANIES

COMPANY	TYPE	ASSESSMENTS COMPLETE including '21/'22 cycle	CASES REVIEWED '21/'22
BT	Telecommunications Operator	1	8
Ericsson	Equipment Vendor	1	8
Facebook (Meta)	Internet	3	8
Google	Internet	4	8
Microsoft	Internet	4	8
Nokia	Equipment Vendor	2	8
Orange	Telecommunications Operator	2	8
Telenor Group	Telecommunications Operator	2	7
Telia Company	Telecommunications Operator	2	8
Vodafone Group	Telecommunications Operator	2	9
Yahoo (formerly Verizon Media)	Internet	4	8

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 Statsautoriseret Revisionspartnerselskab
- DNV
- Foley Hoag LLP
- Osborne Clarke
- Threefold Sustainability
- Venable LLP

4 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 3 of the Assessment Toolkit.

PROCESS REVIEW

The process review consists of a series of questions about the systems, policies, and procedures that companies use to implement the GNI Principles. This section describes the components of the assessment review, as they are outlined in the **Assessment Toolkit**. The individual company determinations that follow provide more information about unique and noteworthy aspects of each company's approach, as detailed in the assessment reports. The information presented for each company is based on titles, processes, and other information as it existed at the time that the assessment was conducted (in most cases during 2021). 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.

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 company's 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.
- Processes to evaluate and, where appropriate, escalate freedom of expression and privacy issues to higher levels in the company.

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 in times 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).

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 and content/network restrictions.[5] According to these reports, and consistent with the Implementation Guidelines, company 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.
- 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.[6]

5 Equipment vendor companies such as Ericsson and Nokia do not receive direct government demands.
6 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.

Each assessment report described the policies and procedures a company has in place to respond to government restrictions or demands that appear overbroad,[7] 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;
- Direct the demanding government to appropriate legal processes, such as Mutual Legal Assistance Treaties;
- Challenge such demands in domestic courts;[8] and/or
- Not comply.

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.

TRANSPARENCY AND ENGAGEMENT

Each assessment report described how companies communicate their general approach to addressing human rights impacts in relation to freedom of expression and privacy to shareholders and stakeholders. As detailed in the Company Determinations, companies disclose this information in a variety of ways including by:

- Detailing the generally applicable laws and policies that require the company to restrict content or communications or provide personal information to government authorities.
- Explaining the company's policies and procedures for responding to government restrictions and demands.
- Publishing reports about the requests and demands that companies receive from governments.
- Engaging 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." Central to the "improvement over time" component is the issuance and follow-up on specific recommendations provided to each company. In this Report we have included, where feasible, in the Company Determinations, high-level examples of some recommendations made by assessors to each company. Additional information and examples of recommendations made by assessors and the Board can be found in the **Improvement Over Time section** of this report.

7 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.

8 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."

CASE STUDIES

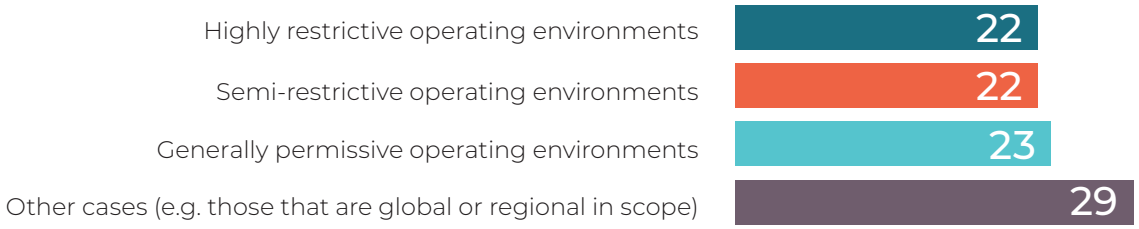
The review of Case Studies provides a window into whether and how companies are implementing the GNI Principles in practice. This section provides aggregate information about the Case Studies that were included in this assessment cycle. Over the assessment period, an individual company may receive thousands 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**.[9] 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.

The publication of this Report was delayed due to unforeseen circumstances. As a result, GNI has chosen to publish the core content of the report first and to subsequently produce a "supplement" that contains descriptions of some of the case studies that were included in this cycle of the assessment. Once that section is published, it will be added to this report and can be found in **Annex 2**.

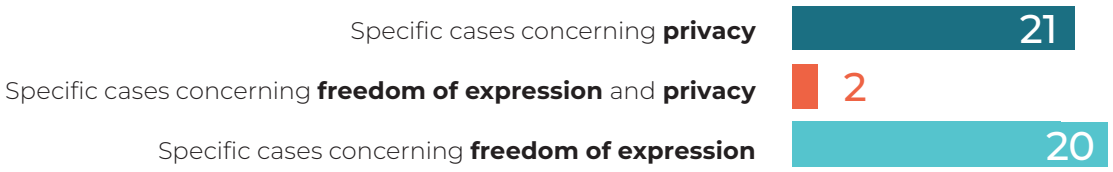
9 See the GNI Case Selection Guidance Summary. For more on the role of the non-company constituencies in case selection, see Section 3.2 of the Assessment Toolkit.

OVERVIEW OF CASES

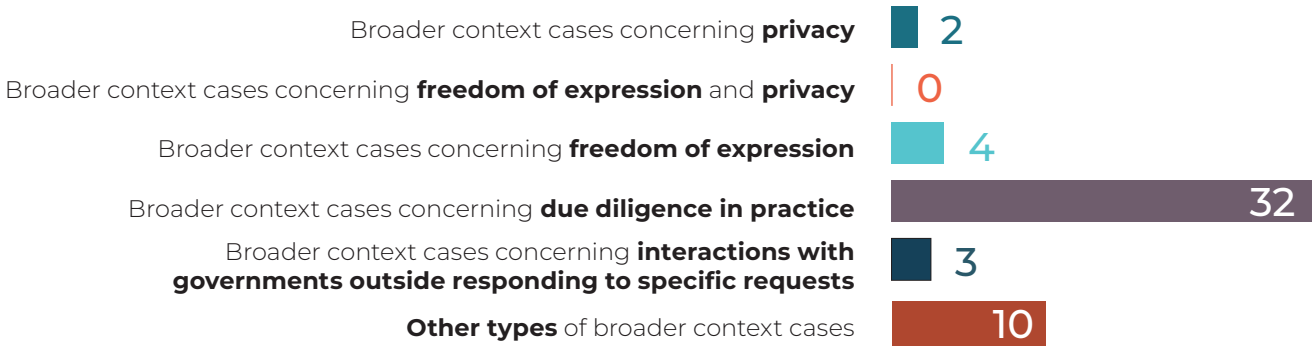
CASES BY OPERATING ENVIRONMENT



CASES INVOLVING A SPECIFIC GOVERNMENT REQUEST: 39



CASES RELATED TO THE BROADER CONTEXT OF COMPANY OPERATIONS: 44



Company Determinations

BT Group[10]

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

ABOUT THE COMPANY

BT Group is the UK's leading provider of fixed and mobile telecommunications and related secure digital products, solutions and services. BT Group provides managed telecommunications, security and network and IT infrastructure services to customers across 180 countries.

BT Group consists of three customer-facing units: "Business" covers companies and public services in the UK and internationally; "Consumer" serves individuals and families in the UK; "Openreach" is an independently governed, wholly owned subsidiary wholesaling fixed access infrastructure services to its customers - over 650 communications providers across the UK.

The majority of BT's services are focused on consumer and enterprise customers in the UK, but the company also provides services in Europe, the Americas and the Asia Pacific. BT's customers in these jurisdictions are typically multinational corporations for whom BT provides networking, cloud, and cybersecurity services. Whilst BT's operations in the UK employ first-party systems and networks, BT's services outside the UK are typically overlaid on local infrastructure owned and operated by other businesses.

GOVERNANCE

The Board is accountable for ensuring that the BT Group's business practices reflect its values and ethics. It delegates oversight of implementation of the GNI Principles to two committees (both co-chaired by Board members):

- The Responsible Business Committee (RBC); and
- The National Security and Investigatory Powers Governance Committee (NSIPGC).

Responsibility for business practice and ethics is also within the remit of the BT Executive Management team (ExCo). The BT Responsible Tech and Human Rights (RT&HR) Team, led by the Group Corporate Affairs Director, oversees implementation of the GNI principles in the UK and other markets in collaboration with leaders from other functions and risk areas. The Group Corporate Affairs Director also attends the RBC and the NSIPGC, and is the sponsor for the RT&HR Team in the ExCo.

Employees complete annual training on Being trusted: our code, BT's ethics code , which emphasizes considerations of privacy and free expression. Frontline personnel undergo tailored training covering the importance of respecting privacy and freedom of expression. Authority to deal with specific types of Law Enforcement Agency (LEA) requests is tied to demonstrating appropriate training and skills (more below).

10 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

DUE DILIGENCE AND RISK MANAGEMENT

BT has processes in place to identify privacy and freedom of expression considerations as part of its Business Impact Assessments (BIA)

When human rights issues are identified, the RT&HR team collaborates with Legal and other stakeholders to undertake an initial Human Rights impact analysis. In doing so, the RT&HR Team considers whether a more detailed, external HRIA is needed to assess and prioritize issues. The RT&HR team also plays a day-to-day role in product and market assessment processes, utilizing the company framework for responsible technology decision making, considering the severity and scope of impacts, and consulting with external lawyers and other experts where necessary. In addition, there are structures in place to identify and address human rights risks within specific markets through the in-country legal teams and the LEA request process.

BT deploys specific tools it will use to mitigate risks identified. These include its standard business terms and conditions (including a requirement for customers to use its services in compliance with international human rights standards and BT's Acceptable Use Policy), and additional restrictions and conditions may be added for higher risk business relationships. If BT has a majority holding in an entity, it requires the entity to adopt its policies, including the Group Privacy Policy, Human Rights Policy and the BT Ethics Code. The Group Corporate Affairs Director has authority to terminate a product or service provision if the human rights impact is considered unacceptable and/or cannot be appropriately mitigated. BT considers its exposure highest in its main UK market because outside the UK it provides over the top services to enterprise customers, for which BT identifies lower levels of privacy and freedom of expression risks.

PRIVACY AND FREEDOM OF EXPRESSION

The companies' policies and practices for responding to LEA requests are built on the License to Operate process, whereby formal training for staff responsible for receiving LEAs is combined with an 'experienced buddy system' for on-the-job training. Capabilities are closely tracked and monitored at a granular, request-type, level.

Global LEA requests are managed by specific, identified in-country personnel. In the UK, where the majority of requests are received, LEA requests are managed by the Global Obligations team. The director of this team, along with the legal director, can escalate issues directly to the NSIPGC, who must approve all non-targeted requests. Where overseas requests raise specific human rights concerns, issues can be escalated via the Global Obligations team. BT's Law Enforcement or Government Agency request processes references the GNI and provides specific tests for necessity and proportionality, along with designating avenues for recipients of requests to raise concerns. All LEA requests and related decision-making are recorded for audit, oversight, and operational purposes.

BT's Privacy & Security by design policies, data minimization policies, and Privacy Impact Assessment Process are intended to ensure compliance with the UK GDPR. Binding Corporate Rules (which were agreed with the Information Commissioner's Office) are also used as safeguards for protecting the transfer of personal data across borders within BT Group and ensure certain common data privacy standards. BT has a dedicated internal privacy team comprising lawyers and compliance professionals who report to its Group Data Protection Officer. They are responsible for ensuring that BT has the right frameworks in place to ensure that it respects privacy and complies with applicable data protection regulations.

TRANSPARENCY AND ENGAGEMENT

BT's Human Rights Policy is available on its corporate website, and BT includes human rights updates in BT Group's Annual Reports. These reports include a section outlining potential impacts on privacy and free expression and examples of how BT mitigates those risks. Annual Digital Impact and Sustainability reports also discuss how BT protects privacy and freedom of expression. BT has an external human rights website setting out its main impacts,

as well as its engagement with GNI, and refers people to human.rights@bt.com to raise concerns.

BT explains the reasons it collects personal information and the ways it uses this information in its Privacy Policies and (in certain circumstances) in customer interfaces at the point of collection. Its Privacy Policy also links to the UK Information Commissioner's Office and informs users of their right to complain to data protection regulators in their country. Users can also ask to see what data is held about them under the Data Subject Access Request process.

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. BT's strong commitment to GNI and human rights was visible among key personnel, including through structures in place to provide effective oversight at a senior level, such as the board sub-committees and the significant responsibility held by the Group Corporate Affairs Director. One area of improvement discussed was that the policies covering freedom of expression and privacy issues could, in some cases, be better formalized and integrated.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. A focus area was better understanding how the company addresses human rights issues in overseas markets and the different products, services, and business relationships that typify BT's presence in these markets. It was noted there could be room to strengthen the emphasis on freedom of expression in addition to privacy in relevant company policies and procedures.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

This was BT Group's first GNI assessment.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Incorporate explicit references to GNI, FoE and Privacy -** Although references to the GNI are made in internal documents and policies, the assessor recommended that BT consider leveraging its membership and commitments to the GNI further with internal stakeholders in training materials and communications. The assessor also recommended that BT consider more explicitly referencing the GNI when engaging in consultations or discussions with government representatives, in order to contextualize its positions and also raise the profile of the GNI.
- **Enhancing Transparency -** The assessor also recommended that BT consider updating its external human rights website to set out its impacts on Privacy and Freedom of Expression, as well as providing a dedicated page for its "Privacy and Free Expression Report".
- **Enhancing Trainint at the Executive Level -** The assessor noted that training Board members on the GNI principles, would empower the Board to take more direct ownership for the strategic oversight of BT's human rights practices.

Ericsson[11]

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

ABOUT THE COMPANY

Telefonaktiebolaget LM Ericsson ("Ericsson"), is headquartered in Sweden and is one of the world's leading providers of ICT infrastructure. Ericsson operates in more than 180 countries with approximately 100,000 employees worldwide. Ericsson is divided into five geographic organizational units, also known as Market Areas, that are responsible for customer sales. The five Market Areas are Europe and Latin America (MELA), North America (MANA), Middle East and Africa (MMEA), North East Asia (MNEA), and South East Asia, Oceania and India (MOAI).

As a network vendor, Ericsson's role is to develop the infrastructure that provides the basis for fixed and mobile communications. Ericsson's main customers are communication service providers and telecom operators. Ericsson provides fixed and wireless telecommunication network equipment and solutions and software, but does not own any operating licenses. In some cases, Ericsson operates networks on its customers behalf, including for fully state-owned operators, but it typically does not deal directly with government authorities. Thus, Ericsson does not usually directly receive or handle governmental requests.

GOVERNANCE

Ericsson's commitment to human rights and how the company addresses issues related to freedom of expression and privacy through the implementation of the GNI Principles can be found in the Code of Business Ethics and the Business and Human Rights Statement. The Board has oversight of matters pertaining to compliance and risk management, including issues related to human rights such as freedom of expression and privacy. Sustainability and corporate responsibility performance and related risks, including issues related to the implementation of the GNI principles, are presented to the Board of Directors annually, or as often as needed. Addressing human rights is built-in into Ericsson's sales process through the Sensitive Business framework. At the time of the assessment, the Sensitive Business Board was made up of members of Ericsson's executive team and senior management and oversaw the execution of the Sensitive Business Framework, including the implementation of the GNI Principles.

DUE DILIGENCE AND RISK MANAGEMENT

Ericsson has integrated human rights due diligence into the organization through the Sensitive Business framework. The framework aims to ensure that business opportunities and engagements are conducted in accordance with international human rights standards. In the Sensitive Business framework, each technology owner is required to answer a set of questions which results in an assigned risk value. Ericsson considers four risk parameters (product, country, customer, and purpose) in all sales

11 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

opportunities. A human rights impact assessment can be triggered at a country or a product level by factors such as re-entry into a country and potentially severe human rights impacts. Additional analysis and action is prioritized based on the severity (including scale, scope, and irremediability) of the potential impacts. In the case of the most severe potential impacts, Ericsson might pursue additional actions such as dialogue with external stakeholders. Ericsson has undertaken several country-specific HRIAs, as well as product-specific HRIAs, including the publication of their Human Rights Assessment Report on 5G technology.

Ericsson ensures the standardized application of the Sensitive Business framework by requiring that each Market Area has a Single Point of Contact (SPOC) responsible for preparing cases for Sensitive Business evaluation. Each SPOC is trained by the Sensitive Business unit at the group level. Ericsson has also developed KPIs to ensure that the Sensitive Business framework is implemented across the company. These include:

- Market Area Sensitive Business Approval Adherence - The Market Areas shall obtain Sensitive Business approval before submitting a proposal.
- Business Area Sensitive Business Technology Evaluation Adherence - The Business Areas shall evaluate all software features.
- Sensitive Business Decision Adherence - Measures the adherence of the Market Areas to the Sensitive Business decisions for each project that has a Sensitive Business decision.

PRIVACY AND FREEDOM OF EXPRESSION IN PRACTICE

Freedom of expression and privacy are addressed across the company through the Sensitive Business framework. In addition, the company has developed Privacy Principles that form the basis of a company-wide global privacy program. This program ensures that privacy is designed into Ericsson's processes, tools, products and services. The privacy program is based on the European General Data Protection Regulation (GDPR) and is adapted where the GDPR level of data protection does not meet the privacy requirements in a particular country.

As a network provider, Ericsson does not typically directly handle government requests, including demands to remove or block online content, requests for user information, or network shutdowns. However, its products and solutions can still impact privacy and freedom of expression. For example, to comply with legal requirements, Ericsson may enable lawful interception functionality through interfaces in its customers' networks. In order to limit the misuse of lawful interception, access to the Ericsson lawful interception interface is secured in a number of ways, including multi-factor authentication, login credentials and certificates, encryption, and digitally signed data. Ericsson will only follow requests and demands coming from legal authorities as agreed in Ericsson's contracts with its customers and defined according to the law. For requests that do not fulfill the agreed contractual terms, Ericsson does not comply with the request and instead escalates the request to the customer following the agreed process. Where legally allowed and where acting as data controller, Ericsson notifies the data subjects in writing after removing or blocking information.

Ericsson encourages employees, suppliers, and other external parties to report conduct that could violate the law, Ericsson's Code of Business Ethics, or Ericsson's Code of Conduct for Business Partners. Compliance concerns can be reported anonymously through the Ericsson Compliance Line by phone or secure website. Ericsson does not accept any discrimination or retaliation against individuals who report compliance concerns in good faith.

TRANSPARENCY AND ENGAGEMENT

Ericsson has a number of different approaches for ensuring transparency in its products and services as well as avenues for stakeholder engagement. The company publishes information on identified risks, actions taken and how it tracks performance on issues related to freedom of expression and privacy in the human rights section of the Ericsson Annual Report. Statistics from the Sensitive Business process are included in the annual Sustainability

and Corporate Responsibility report and are subject to Ericsson's auditor's limited assurance of the information contained in that report. Ericsson also holds an annual NGO and investor stakeholder meeting in connection to the launch of the Annual Report. As part of assessing human rights impacts, Ericsson seeks to understand the concerns of potentially affected stakeholders by consulting with them directly, as well as with independent experts who can bring knowledge or expertise in relation to specific issues, geographical contexts, or other relevant matters. As an equipment vendor, Ericsson also engages proactively on issues that might impact freedom of expression and right to privacy through standardization bodies. Standardization organizations relevant for mobile communications include the International Telecommunication Union (ITU), 3G Partnership Project (3GPP), and Internet Engineering Task Force (IETF). An example of Ericsson's engagement in standards setting bodies is the company's work to advocate for the protection against IMSI catchers in the 3G Partnership Project's work to develop 5G standards.

FOLLOW UP AND IMPROVEMENT

During the assessment meeting, 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 assessor identified Ericsson's systematic approach to addressing human rights, including freedom of expression and right to privacy challenges through its Sensitive Business framework, as one of its main strengths in implementing the GNI Principles. The assessor also highlighted as strengths the publishing of the 5G Human Rights Assessment report, as well as the country-specific HRIAs that the company undertakes. The need to consider network disruptions requests as part of the Sensitive Business framework and formal policies and procedures for mergers and acquisitions were also discussed.

During the Board Review Meeting, which featured representatives from GNI's multi-stakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. This included discussion on the company's approach to identifying country-specific risk, avenues for the company to identify more real-time shifts in situations where human rights are impacted, ways to integrate network shutdowns into the company's risk identification framework, as well as approaches to strengthening stakeholder engagement. The importance of bringing a holistic perspective to understanding human rights risks across the technology ecosystem was also highlighted.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

This was Ericsson's first GNI assessment.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Managed Services -** The assessors recommended that Ericsson continue with efforts to establish a new policy framework for managed services related to governmental requests.
- **Mergers & Acquisitions -** The assessors recommended that Ericsson strengthen procedures and due diligence requirements with respect to human rights in connection to M&A activities.
- **Training -** The assessors recommended that Ericsson identify key job roles in scope for human rights training and strengthen specialized training on human rights for those roles.

Google[12]

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

ABOUT 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, Google Cloud, 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 device business. As of Q2 2022, Google had over 174,000 employees. A global company, Google's headquarters is located in Mountain View, California, and it has 85 offices around the world, primarily in North America, Europe, South America, and Asia.

Google is a subsidiary of Alphabet Inc.

GOVERNANCE

Senior management oversees the implementation of the GNI Principles at Google and provides regular updates to the Board on relevant issues, including risks to human rights. The Board provides oversight and responds to concerns raised by senior management, including through review and discussion of significant regulatory matters that may impact human rights.

The 2018/19 assessment detailed a "matrix"-like personnel network within Google designed around product, jurisdiction, and functional areas who contribute to strategy and operations that protect user rights of freedom of expression and privacy. During the review period, the company took steps to build out human rights infrastructure with direct participation of and oversight by senior personnel. The Global Head of Human Rights has a team focused on providing education, risk analysis, and guidance on human rights issues, and ensuring the company maintains its commitment to the GNI Principles across the various departments and levels at Google. There are dedicated teams within legal, government affairs and public policy, and trust and safety responsible for responding to government demands; dedicated product and regional counsel who may identify and participate in addressing risks to freedom of expression or privacy in product design or operation, and in specific regions; and policy experts for specific products, countries, and functional areas who identify and address risks to freedom of expression and privacy to Google's operations. During the review period, the company created the Human Rights Executive Council (HREC), which consists of high-level leaders across the company who set direction and review specific threats and issues related to human rights, working with the Global Head. The HREC meets quarterly, and includes a working group on Assessments and Disclosures that meets separately and reports back to the HREC.

12 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

Google

Google provides targeted training for all levels of personnel based on job function. This includes educating employees on evaluating risks to privacy and freedom of expression and how and when to escalate issues. All employees are made aware of the company's freedom of expression and privacy commitments through the required code of conduct training, which includes information on raising concerns through an anonymous helpline. In addition, the company provides intensive, deep-dive training on its human rights commitments, due diligence processes, internal processes, and escalation channels for relevant frontline teams, which is supplemented with broader education and efforts to raise awareness internally, such as the annual civil and human rights symposium.

DUE DILIGENCE AND RISK MANAGEMENT

Google personnel, led by the Google Human Rights Program (GHRP) conduct internal due diligence on an ongoing basis, including for specific jurisdictions, and for new products, new features, laws, and policies that may impact freedom of expression and privacy. Product-specific counsel are part of the development lifecycle of any new products or features, and serve as the initial eyes and ears for raising potential risks to freedom of expression or privacy, consulting with internal guidelines and relevant teams as needed. Product and regional counsel, in coordination with GHRP staff, assess risks to freedom of expression and privacy in new jurisdictions as laws change or evolve. Acquisitions are generally integrated into Google operations, thereby becoming subject to product and service policies and procedures, and other business partnerships typically utilizes contractual terms which where relevant require adherence to Google's freedom of expression and privacy principles.

Where this ongoing HRDD and review of potential human rights issues may surface products or jurisdictions with higher risks to human rights, Google may use a formal Human Rights Impact Assessment. The GHRP oversees completion of all HRIAs, whether conducted in-house or with external parties, and ensures results are shared internally, including providing recommendations for leadership where appropriate. Google relies on regional and local counsel, product and policy experts, human rights consultants, and relevant third-party inputs to inform HRIAs.

Google takes a multi-faceted approach to mitigate risks identified through due diligence and other ongoing evaluations, including considering whether products can be offered globally, identifying potential mitigation measures, and addressing known challenges in particular jurisdictions, seeking to make products as accessible as possible while abiding by local laws and requirements. Google seeks to engage with governments around the world to resolve challenges that impact freedom of expression and privacy, also involving local trade associations, NGOs, companies, international organizations and other experts to impact change.

FREEDOM OF EXPRESSION AND PRIVACY IN PRACTICE

The Data Disclosure Strategy Team (formerly known as the Law Enforcement and Information Security Team") designs, implements, oversees, and revises policies for responding to government requests for user information, while requests for content removals or restrictions are handled by separate teams at YouTube and the rest of Google. Google requires governments to submit requests in writing and reviews the legal validity of each request based on authority and specific application of local law and may push back on those that appear vague. If sufficient clarification is not met, Google must return or deny the request.

For removal requests, Google will review these requests in light of international human rights standards and ensure that legal requirements for content moderation are narrowly interpreted to prevent inadvertent precedent setting. Google has policies that ensure action on content is only taken when clearly required and the scope of the action is limited to the extent required by law, including but not limited to when the territorial scope of laws or requests are ambiguous, Google will narrowly interpret removal requests to avoid unnecessary removal. If legal requirements necessitate removal, Google has a policy that content is only removed in the affected jurisdiction.

Google

Google's Privacy Policy clearly describes the user information collected and how it is used, shared, and disclosed. The Privacy Policy covers all products, including some special circumstances with specific guidelines on those changes.

Google retains detailed records of all government requests, and ongoing conversations between specialized teams are used to monitor trends and region-specific issues. Google publishes data about government requests and the type of content that triggers approval or denial in its Transparency Report, and encourages governments to tailor requests in a way that does not infringe on freedom of expression and privacy. Google encourages laws and regulations consistent with international law and standards by meeting regularly with law enforcement and national security organizations worldwide as well as regulators and policymakers, to build channels for open dialogue and discussing human rights issues.

Google assesses risks associated with individual jurisdictions when determining where its data is physically collected, stored, and retained. The nature of data collected or processed in certain jurisdictions changes based on these risks, informing Google's approach to expanding to new jurisdictions and implementing new compliance processes.

TRANSPARENCY AND ENGAGEMENT

The Google Transparency Report describes the company's approach to government removal and user data requests and discloses the company's response to requests. The report covers various regions where government conduct may impact freedom of expression or privacy. Google executives and staff also issue public blog posts and have testified regarding freedom of expression and privacy issues globally. Individual product teams provide their own statements of values (e.g., YouTube "Four Rs"; Blogger content policy). Google also has a **webpage** dedicated to its human rights commitment as part of its "About" page, and launched an online Safety Center with best practices, tips, and other tools. In addition to transparency reporting within Google's Transparency Center, Google provides information on the laws and policies related to the company's restriction and disclosure of content and communications through multiple channels, such as Google Transparency Reporting, Community Guidelines, Privacy Policy, Terms of Service, and the Legal Removals page.

Google's standard practice is to notify users when content is removed due to a government request by emailing the user and placing a notice on the webpage where the content was previously displayed. Any visitors who attempt to view the content will receive the same notice. Google will also send these removal notices to **Lumen**, a Harvard University data removal transparency project. Google will not provide these disclosures when restricted by court order or law, such as in an ongoing criminal investigation. When data is disclosed to a government agency pursuant to legal process, Google will notify the user whose data was disclosed, unless the law specifically and clearly restricts user notification.

Google regularly meets with NGOs, human rights organizations, and regulators to discuss human rights issues. Additionally, the company participates in human rights events like the Freedom Online Coalition meetings, the Internet Governance Forum, and RightsCon. Engaging with governments to address actual and potential impacts to freedom of expression and privacy is a core function of Google's Government Affairs & Public Policy (GAPP) Team, in collaboration with various teams, including Legal, Trust & Safety, and Compliance. Examples of legislative discussions with governments that highlight the letter and spirit of the GNI Principles include Google's feedback on: Canada Online Harms Act; EU Digital Services Act; and the India IT law. Google encourages government- to -government communication, including through engagement with the engagement with the Division of Democracy, Human Rights, and Labor (DRL), and work closely with various international organizations to promote the rights to freedom of expression and privacy, including dedicated staff for specific organizations like the UN, Council of Europe, OECD, etc.

Google

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 the steps the company has taken to further build out infrastructure to expand and entrench its multi-pronged approach to tackling human rights challenges in the short and long-term. It was noted that the company can sometimes better articulate this approach publicly, including communicating information on specific cases, stronger communication from executives, and creative approaches to doing so, including with trusted organizations.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. There was discussion about how the company prioritizes countries for government engagement and human rights risk management. There was discussion of avenues for scaling stakeholder engagement efforts with the company's global footprint, including resource considerations. There was discussion of how the company approaches the concept of public interest, which plays a role in the company's approaches to responding to government demands and content decisions, and related transparency.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessors reported that Google formalized its Human Rights program and appointed a Global Head of Human Rights who currently leads the Human Rights program, and reports directly to a Vice President level executive. The company also implemented a previous recommendation to provide more updates on human rights activities by introducing an inaugural symposium, available to a broad range of Google employees across all organizations represented in the HREC, which the Human Rights program plans to make an annual activity. Finally, in response to another recommendation, the Human Rights program has developed training to provide a high-level overview of human rights policies and processes, which has been implemented within the Trust & Safety and Government Affairs and Public Policy teams. This training will be expanded further as the program develops.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Continued Development of Structure and Capacity -** The assessor made a number of related recommendations based on and intended to bolster progress made during the assessment period, including continuing to build the capacity and scale of the GHRP, considering ways that the HREC can engage with other internal leadership bodies, and focusing resources to support management of crisis issues and circumstances.
- **Expanding Transparency and Communication -** The assessor praised Google's engagement in various human rights initiatives, efforts to educate users and other stakeholders about its services and policies, and its approach to risk assessment, but noted that higher level, more frequent, and more detailed communications regarding its dedication to the UNGPs and the GNI Principles, could help increase awareness among and strengthen relationships with civil society and other stakeholders. Noting the challenges that often arise with public transparency in the context of operations in sensitive environments, the assessors recommended using trusted stakeholder relationships to disclose and discuss strategies and developments instead.

Meta[13]

ABOUT THE COMPANY

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

Meta builds technologies to help people connect, find communities, and grow businesses. This includes through mobile devices, personal computers, virtual reality, wearables, and in-home devices. Meta's services are available across the globe and its operations are divided into two key segments: the Family of Apps (Facebook, Instagram, Messenger, and WhatsApp) and Reality Labs (augmented and virtual reality products).

GOVERNANCE

Meta's commitment to the GNI principles can be found in the company's Human Rights Policy, which also includes commitments to the United Nations Guiding Principles on Business and Human Rights, as well as other human rights principles and international standards. Meta's Board provides strategic oversight of the implementation of the **Human Rights Policy** ("the Policy") through the Audit and Risk Oversight Committee (AROC). The President of Global Affairs and Chief Legal Officer are co-sponsors of the Policy.

The Policy is implemented across the organization by the Human Rights Team. A number of mechanisms are in place to enable the implementation of the Policy including human rights due diligence frameworks, operational playbooks, guidelines, cross functional advisory and decision-making groups, and multi-platform tools. Training opportunities on the Policy, including the GNI Principles and Implementation Guidelines, are provided across teams in the organization.

DUE DILIGENCE AND RISK MANAGEMENT

Meta has in place a number of processes through which human rights impacts are identified and addressed. Meta uses the UN Guiding Principles Reporting Framework, along with the United Nations Guiding Principles guidance on severity, to prioritize human rights concerns and impacts. When salient human rights impacts are identified, Meta will consider appropriate steps, which can include undertaking a formal HRIA. Examples of instances when Meta has carried out HRIAs or other forms of human rights due diligence include when considering establishing a physical presence, launching new products or features with potential human rights implications, or where Meta's services might result in human rights impacts in a specific context. To help the company identify context specific human rights concerns, Meta maintains an "**At Risk Country Prioritization Framework**" that identifies and prioritizes human rights risks across contexts. After human rights due diligence is carried out, Meta's Human Rights team works to incorporate recommendations into relevant products, policies, and processes.

13 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

Meta has formal processes in-place for the escalation of issues and decisions related to human rights, including privacy and freedom of expression, by all employees which permit escalation up to the VP and CEO level if needed. For example, employees can raise concerns through the Privacy Review process, the Content Policy Forum, and the Trust and Safety product counselling processes. The internal Human Rights Team wiki, Meta's **Code of Conduct**, and Meta's Whistleblower and Complaint Policy also provide employees with pathways and information on how to raise concerns.

FREEDOM OF EXPRESSION AND PRIVACY

Meta has in place frameworks and guidelines to respond to government requests for **disclosure of user data** and **content restrictions**, which have been informed by the GNI Principles. These frameworks include commitments to evaluate government requests for user data and content restriction under international standards, as well as company principles, policies, and applicable law. Meta also publishes operational guidelines for law enforcement and other governmental officials seeking information from Meta.

Meta has a Law Enforcement Response Team that reviews and evaluates government requests for user information. The company **commits** to only comply with government requests for user information where it has a good-faith belief that it is required to do so by law. Unless prohibited by law, in exceptional circumstances, or when it would be counterproductive, Meta will notify users about a request for their information before disclosing it. With respect to privacy more broadly, Meta's data policies detail what personal information the company will collect from users and how it will be used. Meta's Privacy Centre and Privacy Basics portals provide users with tools and information to control and manage their personal data. Meta's data policies also provide information on how users can contact the Privacy Team, and where relevant, the Data Protection Officer and Data Protection Authority with complaints. Further, the Global Privacy Operations team receives and responds to privacy-related complaints, which can be submitted online or through the mail.

Meta's **policies** for responding to government requests for content restriction are overseen by a cross-functional group that includes members of the Human Rights, Regulatory Compliance Policy, and Legal teams. If content violates Meta's **Community Standards**, the company will remove the content globally and notify the user. If Meta receives a lawful governmental request for removal of content, the company will carry-out further legal analysis and due diligence and may push back on the request if it determines that it is overly broad or inconsistent with international standards. When Meta takes action on content based on a government request, the company may restrict access in relevant jurisdictions and will seek to provide notice to users via a direct in-app notification. Meta also provides a notice to anyone attempting to directly access the content informing them that the content is not visible due to legal requirements. Meta maintains grievance mechanisms for individuals whose content has been removed for violating its Community Standards through in-product appeals processes. Individuals can also submit cases to the Oversight Board.

TRANSPARENCY AND ENGAGEMENT

Meta has multiple forms of transparency in place. Through the **Transparency Center**, Meta reports on how the company responds to government requests for disclosure of user data and content restrictions. This includes information on the number of pieces of content, the types of content restricted, and the legal basis for the requests. In July 2022, Meta published its first **Annual Human Rights Report** and launched a dedicated Human Rights **website**.

Meta will engage stakeholders, including governments, on legal and regulatory developments impacting privacy and freedom of expression. In addition to GNI, examples of organizations and entities that Meta engages with include the Asia Internet Coalition, the Organization of American States Special Rapporteur on Freedom of Expression, the Reform Government Surveillance Coalition, and the UN B-Tech initiative.

FOLLOW UP AND IMPROVEMENT

During the assessment meeting, 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 assessor identified Meta's work to ensure the GNI Principles form part of a wider cultural commitment to human rights as one of the main strengths and successes in implementing the GNI Principles. The assessors noted areas of growth in the company from the last assessment, including the appointment of a Human Rights Director, its first dedicated Human Rights Report, and its new Human Rights Policy.

During the Board Review Meeting, which featured representatives from GNI's multi-stakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. This included discussion about the process followed by the company for identifying and prioritizing country specific risks as well as the different tools the company uses and avenues for engaging with local experts and stakeholders. Input was also provided on ways the company can increase transparency on HRIAs, improve the accessibility and implementation of the company's Terms and Conditions to a global user base, and implement the GNI principles across business lines.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessor reported on steps Meta has taken to carry out recommendations made in the Third Assessment Cycle, including those related to effective human rights due regarding third party relationships, integration of human rights due diligence into company risk management, ensuring ongoing leadership and Board oversight and ownership, and improving training and awareness around the GNI principles. The assessor highlighted efforts to ensure consistency of relevant policies and procedures across the Family of Apps; transparency improvements for users regarding the Company's data collection, storage, and retention practices; and expansion of the situations where human rights due diligence may be conducted.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Documenting Processes & Decisions -** The assessors made recommendations on how Meta could map out and provide clarity internally around relevant HRDD and HRIA processes. Related recommendations discussed how spot checks or internal audits to review relevant processes related to responses to government demands could support Meta's iterative, internal approach to policy development.
- **Transparency -** The assessors recommended that Meta consider the technical and practical feasibility of providing greater granularity and detail related to government requests in its Transparency Center.
- **Training -** The assessors made recommendations on how Meta could expand its internal training on GNI-relevant scenarios, policies, and processes, including consideration of tailored training of senior decision makers.

Microsoft[14]

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

ABOUT 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 every organization on the planet to achieve more. The company employs some 181,000 personnel worldwide and operates in 190 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 free expression and privacy. Examples of such services include Microsoft's Bing search engine, its LinkedIn professional social networking service, its Skype VOIP communications platform, and its free Outlook.com webmail service, among others.

GOVERNANCE

Day-to-day oversight of Microsoft's implementation of the GNI Principles is the responsibility of the Vice President and Deputy General Counsel, who leads the Human Rights team within Microsoft's Corporate, External, and Legal Affairs (CELA) department. They also have direct access to Microsoft's President and Vice Chair and escalate matters to the President and other CELA executives as needed.

Microsoft's Board of Directors provides strategic oversight of the company's fundamental commitments. This includes the company's commitment to respect human rights as exemplified by its commitment to and implementation of the GNI Principles. The Environmental, Social, and Public Policy Committee of Microsoft's Board of Directors has primary oversight over GNI implementation. Both this Committee and the larger Board of Directors receive briefings on freedom of expression, privacy, and other human rights matters quarterly from the President and Vice Chair.

Microsoft's commitment to implementing the GNI Principles is embodied in two core policy documents: its public-facing Global Human Rights Statement (which addresses both freedom of expression and privacy), and an internal Freedom of Expression Policy document. The Global Human Rights Statement was updated in December 2022. Microsoft's CELA department is responsible for driving the implementation of these policies (and through them the GNI Principles) across the company and its various business groups. Each business group at Microsoft is supported by a dedicated CELA team that provides front-line support on the full range of legal and public policy issues (including freedom of expression, privacy, and other human rights) encountered in the development and delivery of products and services. Front

14 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

line teams are supported by CELA specialists. CELA front line teams are tasked with identifying salient legal issues and risks, and escalating to CELA Human Rights Team and other SMEs for support. All CELA personnel are provided with appropriate training on the identification of risks and the procedures to escalate issues to CELA subject matter experts.

The CELA human rights team is responsible for providing human rights training and providing ongoing support to frontline personnel who handle government requests. The company's senior management (up to and including the President and Vice Chair) receive regular briefings from the CELA Human Rights team on freedom of expression and privacy issues. There are escalation paths within these specific CELA teams and throughout CELA when issues of first impression arise in relation to the rights to free expression and privacy, and also in circumstances where difficult choices need to be made.

DUE DILIGENCE AND RISK MANAGEMENT

Microsoft conducts human rights due diligence to determine whether there are issues and questions that merit further or deeper evaluation. Product related risks that are considered include the nature of the product or service under development, the categories and quantities of data that the product or service would require or generate, and other similar considerations. Market-related risks that are evaluated include the legal framework and human rights practices of the jurisdictions in question.

Key considerations the company takes into account in identifying human rights risks and impacts include the nature of the services, the types of user data or content involved, and the laws and human rights practices of the jurisdictions involved. Microsoft prioritizes among the free expression and privacy issues identified via its due diligence efforts based on salience or, in the case of positive human rights impacts, based on its evaluation of where the potential to advance human rights is at its greatest.

The salience of such risks is assessed by determining the likelihood that government entities may direct demands at Microsoft for user data or content restriction that are inconsistent with the rights to privacy and free expression, and the severity of the resulting rights impacts.

When issues or questions require further evaluation, Microsoft conducts human rights impact assessments to develop prevention or mitigation measures. Microsoft conducts certain HRIAs in-house, and engages external experts to assist with the conduct of such HRIAs when warranted by the scope and nature of the exercise. In all cases, Microsoft looks to a variety of information in conducting HRIA. In appropriate cases, Microsoft will go beyond public sources to engage with respected third parties and may seek an expert legal opinion from an in-house or external lawyer qualified in the jurisdiction. The results of HRIAs that the company conducts are incorporated back into its business in a variety of ways, based on the conditions that triggered the HRIA in the first place, but could result in policy initiatives, approaches to offering particular services or features in a new market, or potentially including or excluding certain features in certain markets for particular end users.

Microsoft mitigates the free expression and privacy risks identified in its human rights due diligence processes through a variety of means, depending on whether the risk is posed by the nature of its services, the types of user data or content involved, or the risks associated with offering its products or services in a particular jurisdiction. In some circumstances, Microsoft might undertake design or other mitigation measures in the features or capabilities of a product. For country specific risks, it might adjust or adapt services or features it offers to mitigate such risks.

Finally, 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 Global Human Rights Statement and its specific policies and procedures to implement the GNI Principles.

FREEDOM OF EXPRESSION AND PRIVACY IN PRACTICE

Microsoft's internal Freedom of Expression Policy (hereinafter "FOE Policy") guides the company's response to government demands that implicate the right to free expression. The FOE Policy stipulates that government orders should be lawfully authorized, binding, and in writing, unless otherwise authorized under the law. The FOE Policy sets out as objectives that Microsoft should comply in a manner that minimizes the impact on freedom of expression, and provides relevant information to users, including notice where specific content has been blocked or removed in response to a government order, unless prohibited by law.

The CELA Law Enforcement & National Security ("LENS") team, and for LinkedIn the Law Enforcement Response Analyst ("LERA") team, are responsible for the handling of government requests for user data, and the implementation of the company's policy for handling such government requests. That policy sets out that Microsoft's approach to reviewing such requests to ensure they follow applicable legal process, are focused on specific accounts and identifiers, and that where the company responds it only provides the data specified in the order.

In deciding whether and where to collect and store certain categories of personal information, Microsoft considers the nature of the services, the types of user data or content required to provide the services in question, and the laws and human rights practices of the jurisdictions involved. These considerations may lead the company to adjust, adapt, limit or avoid the operation of some types of services or features in certain jurisdictions, or to store user data in jurisdictions with adequate protections for the rights to privacy and free expression.

TRANSPARENCY AND ENGAGEMENT

Microsoft sets out its overall commitment to respect human rights and its policies on government demands through its Global Human Rights Statement. In addition, the company provides transparency regarding the personal information the company collects, uses, and shares through its Privacy Statement. Microsoft also communicates its approach to emerging privacy and free expression challenges through the "Microsoft on the Issues" blog.

Microsoft provides transparency regarding its practices in handling government requests through the publication of four different transparency reports, each of which includes an overview of the company's practices for handling government requests, and frequently asked questions detailing applicable laws and policies that require the company to remove content or provide user data pursuant to specific government demands or requests. Microsoft is also committed to providing notice to its users when content is removed or blocked or their data is sought in response to a government request, unless prohibited by law.

Microsoft engages extensively with governments to advocate for the rule of law and the appropriate protection of all human rights, including the rights to privacy and free expression. Examples of Microsoft's engagement include its advocacy in favor of six principles for international agreements to govern law enforcement access to data, its call for government regulation of the use of facial recognition technology (especially in the government surveillance context), and the company's participation in GNI, the multistakeholder Advisory Network for the intergovernmental Freedom Online Coalition, and in partnership with other companies in the technology industry.

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 assessor emphasized the commitment to the GNI Principles at the highest levels of the company, as well as the company's well-developed processes for HRDD and interacting with governments in the context of demands and requests.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. There was discussion of the ways government demands might or might not apply to Microsoft's various services and offerings. There was also discussion of the respective roles and responsibilities of governments and companies regarding the provision of remedy in the context of government demands that impact users' rights.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessors had previously recommended that Microsoft and LinkedIn consider ways to promote greater collaboration and shared learning between relevant teams, and reported in this assessment that Microsoft and LinkedIn share information and learnings on an ongoing basis on handling government requests.

Nokia[15]

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

ABOUT THE COMPANY

Nokia is a global supplier of network equipment that operates or sells products in approximately 130 countries. Nokia's business focuses on the development, sale and support of critical network technology, and the licensing of intellectual property. Nokia focuses primarily on business-to-business transactions but also has a business engaged in brand and technology licensing to business-to-consumer companies.

Nokia has four business groups: Mobile Networks, Network Infrastructure, Cloud and Network Services, and Nokia Technologies.

GOVERNANCE

Nokia's **Human Rights Policy** and implementation of that Policy, including implementation of the GNI Principles, is managed by Nokia's Corporate Affairs, Environmental, Social, and Governance (ESG) function. Oversight of ESG, including Human Rights, sits generally with both the Board of Directors and Executive Management. The Board reviews the ESG strategy annually and specific issues as needed. The Group Leadership Team (GLT), chaired by the President and CEO and appointed by the Board, reviews and approves implementation of and changes to sustainability-related policies (including the Human Rights Policy). Nokia's Chief Compliance Officer (CCO) has oversight of Nokia's adherence to GNI principles and presents regularly to the Board and quarterly to the Audit Committee. The Head of Human Rights is the designated functional expert for Nokia's Human Rights Policy, reviewing policies and procedures, and developing and delivering relevant training and communications.

The **Code of Conduct** provides direction to its employees and business partners and defines the principles of ethical and compliant business practices, including basic legal guidance, key standards, and information about how Nokia works with suppliers. It also includes summaries of the 14 key business policy statements that provide guidance on proper ethical conduct. The Code of Conduct is part of Nokia's mandatory ethical business and corporate governance compliance training. Legal & Compliance (L&C) and Corporate Affairs provide additional targeted training for specific audiences in the company, including training on HRDD processes led by the Human Rights team.

DUE DILIGENCE AND RISK MANAGEMENT

In Nokia's view, salient threats to privacy and freedom of expression related to the company and business result largely from the potential misuse of its technology. At an operational level, the primary way in which Nokia manages this risk and implements the GNI Principles is through its

15 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

Human Rights Due Diligence (HRDD) process, which is embedded into the company's 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.

The sales approval process includes mandatory inputs on human rights considerations related to customer, country, and products, review of which is led by the Head of Human Rights or supporting in-house Legal Counsel, as well as triggers for further escalation. Potential issues are also often surfaced directly to the HRDD facilitators by colleagues even before the formal review in the sales approval process. The most challenging issues and decisions are escalated to a cross-functional HRDD advisory panel or the HRDD Governance council, which includes representatives of the company's leadership team.

Nokia requires its distributors, resellers, and value-added partners to adhere to Nokia's Commercial Third-Party Code of Conduct. Among other provisions, the Code requires Nokia's third-party partners to share Nokia's commitment to human rights and to "act accordingly." Nokia undertakes extensive HRDD and imposes stringent human rights requirements when using third-party distributors and contractors to sell and install products in countries in which the company does not have a business presence.

FREEDOM OF EXPRESSION AND PRIVACY

Nokia supplies telecommunications equipment and services (including managed/maintenance services) mainly to mobile and fixed operators, with increasing sales to enterprises. Accordingly, unlike mobile operators or internet companies, there are limited circumstances when Nokia holds subscriber information (e.g., when performing service-related work). Nokia commits to only provide equipment enabled with lawful intercept capabilities consistent with globally-recognized standards such as those developed by the 3rd Generation Partner Project (3GPP) or the European Telecommunications Standards Institute (ETSI) and where customers might have a legal obligation to provide such capabilities. Furthermore, Nokia will not engage in any activity relating to active surveillance technologies, such as storing or analyzing intercepted data. Assessing risks of interception and surveillance functionality is part of the company's HRDD sales approval and product development processes. The HRDD process does not consider financial aspects of potential sales, focusing instead on the potential for product misuse.

The company implements a comprehensive, group-wide privacy management program, based on relevant laws, best practices, and standards, and aligned with company policies and processes. Nokia's Privacy Statement discloses to customers the personal data it collects and details how it processes, stores and disposes of that data, as well as the instances in which it may be required to disclose such information to third parties. In addition, the Human Rights Policy states the company will not knowingly provide technology or services for purposes of limiting political discourse or blocking legitimate forms of speech.

TRANSPARENCY AND ENGAGEMENT

Nokia publishes an annual **sustainability report** through which it shares its approach, procedures, activities, and risks related to human rights, including details about its privacy and security activities and information on its commitments to the GNI Principles. The report includes anonymized case studies describing Nokia's human rights decision-making and provides context regarding the types of issues the company encounters. Nokia uses a variety of additional channels to communicate to external and internal stakeholders on human rights, including intranet updates and news stories, blog posts, training sessions (including specialized training on issues such as AI and ethics/human rights), other internal releases, and social media channels. Nokia also participates in numerous industry groups, expert initiatives, and multistakeholder coalitions such as GNI, and frequently engages with relevant government entities, in particular with its home government in Finland.

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 assessors highlighted the company's strong human rights culture, noting that many issues are flagged and addressed informally even prior to surfacing during formal processes. They also praised the robust HRDD processes encompassing relevant functions across the company with strong escalation mechanisms. As an area for improvement, the assessors noted that issues managed exclusively through informal channels can contribute to gaps in documentation.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. There was discussion on avenues for further clarifying and strengthening the company's procedures related to reviewing past HRDD decisions. It was also noted that discussions on lawful interception and its related risks would benefit from improved external stakeholders' understanding of the distinctions between passive and active interception of communications, a topic of past and potential further learning within GNI.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessors reported that, in response to a previous recommendation around assessing the human rights impacts of new technologies, Nokia created a working group on "Responsible AI" and was in the process of obtaining input from a large group of external stakeholders to help establish its overall approach to AI. In addition, the company has a formalized process to screen new technologies emerging from Nokia's research and development teams, which facilitates risk mitigation at the level of the technology as a whole. Once the technology has been developed, the company's HRDD process captures risks related to specific use cases.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Action Reviews of Decision Making -** The assessor recommended that Nokia conduct a post-mortem review of select decisions in order to determine whether the company has any identifiable gaps or blind-spots. Such a review process, conducted at least annually, could assist the company in identifying any systematic issues so it can appropriately adjust its policies and diligence processes.
- **HRDD Documentation -** The assessor recommended that Nokia consider establishing a formal documentation policy for its Human Rights Due Diligence decisions, including consideration of documenting informal decision-making, pointing out that doing so would also assist it in the recommended postmortem reviews.

Orange[16]

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

ABOUT THE COMPANY

Orange is an international telecommunications operator with sales of 43.5 billion euros in 2022 and 136,000 employees worldwide at 31 March 2023, including 74,000 employees in France. The Group has a total customer base of 288 million customers worldwide at 31 March 2023, including 243 million mobile customers and 24 million fixed broadband customers. The Group is headquartered in France and is present in 26 countries in Europe, the Middle East and Africa.

Orange is also a leading provider of global IT and telecommunication services to multinational companies under the brand Orange Business. In December 2019, the Group presented its "Engage 2025" strategic plan, which, guided by social and environmental accountability, aims to reinvent its operator model.

GOVERNANCE

The Board of Directors and the Executive Committee provide oversight of Orange's implementation of the GNI Principles. Each year, the Board approves the company's Vigilance Plan, which details measures to prevent and mitigate serious violations of human rights and fundamental freedoms and risks to health and safety and the environment in accordance with the French Duty of Vigilance Law. The integration of freedom of expression and privacy risks brings an additional level of internal controls and oversight of GNI issues, including for local Orange entities (i.e., business groups and country operations) and other business relationships.

The Group CSR directorate has lead responsibility for the preparation of the Group's Vigilance Plan and the operational monitoring of its implementation and associated reporting, reporting back annually to the Executive-level Ethics and Sustainable Performance Committee (ESPC). The Group CSR team works in collaboration with the Group Secretary General and Chief Legal officer, the Data Protection Officer, and the three "Zone Directors" (to whom local CEOs report) to share best practices and ensure compliance with relevant internal controls. During the reporting period, the company appointed a Group Vigilance Plan Manager to oversee implementation, as well as various local counterparts responsible for risks in local entities.

Orange provides training for all personnel to receive a "visa" on its corporate social responsibility commitments. In 2021, Orange started to roll out dedicated training on the Vigilance Plan, first to employees in Orange entities with responsibilities relating to the implementation of the Plan, followed by awareness sessions to wider personnel. All employees also have access to general data protection and privacy training.

16 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

DUE DILIGENCE AND RISK MANAGEMENT

Orange's company-wide human rights risk identification and assessment relating to freedom of expression and privacy is conducted using the Orange Group Risk Management methodology and is integrated into its general Group risk mapping and Group Vigilance Plan risk mapping. On a yearly basis, Orange CSR team carries out prioritization of CSR and human rights issues through a materiality assessment. This process is informed by stakeholder engagement. Orange's 2021 materiality assessment included input from stakeholder dialogues that were launched in 2020 in Sierra Leone, Poland, Tunisia, Spain, Jordan, France, Mali, and Guinea Bissau.

The company integrates HRDD into various company processes, including the Time to Market Process linked to all new product launches. Products which require handling of personal data must undergo a privacy risk assessment called EvalRisk, which examines the legal basis for data processing, any potential third-party access to data, and potential cross-border data transfers, among other issues. Regarding other business relationships, Orange's Responsible Purchasing Steering Committee, together with Orange risk managers, scores suppliers based on their potential human rights risk, with a supplemental assessment and potential mitigation measures required for suppliers that may represent high risks. When new merger and acquisition (M&A) activity is considered, the company considers questions relating to privacy and data protection on a case-by-case basis.

Each Orange entity must, on an annual basis, identify which human rights risks are of greatest risk for them and establish controls and mitigation plans to address the risks identified. Plans must be approved by the relevant Board of Directors, and additional oversight and review is provided by the Group Vigilance function. In addition, group internal audit carries out audits dedicated to compliance with the Duty of Vigilance law in one to two entities per year. Identification and prioritization of country risk is informed by third-party human rights risk assessments, which are also mapped against the election schedule for country entities. Per Orange's Data Protection Policy, each entity is responsible for mapping local data protection laws and ensuring compliance, and the company maintains a corresponding database.

At group level, Orange complements its audits of its upstream value chain by relying on the power of action of the JAC (Joint Alliance for CSR), of which it is a founding member. This association aims to verify, develop, and assess Corporate Social Responsibility (CSR) implementation across the manufacturing centers of suppliers in the ICT industry.

FREEDOM OF EXPRESSION AND PRIVACY

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 related parts of the GNI Implementation Guidelines. This document defines governmental demands affecting a large number of customers simultaneously as a major event that must be escalated to the respective Zone Director, to the Group CSR department, regional CEO, and to the Group General Secretary (Chief Legal Officer). The process is shared with all local entities and CEOs via Zone directors, and each entity has a dedicated Government Obligations Manager or a Head of Government Obligations to manage and process government demands and serve as a point of contact for authorities. They must also keep record of requests to inform aggregated transparency reporting at Group level.

During this assessment period, Orange has introduced a new data protection policy for the Group. This policy is GDPR aligned, and its standards are applied across all Orange entities (with due consideration for local law requirements). The company implements a Personal Data Protection governance program and manages a network of data protection officers.

TRANSPARENCY AND ENGAGEMENT

Orange publishes **several reports** that describe its approach to privacy and freedom of expression. This includes a thematic data sheet on human rights updated annually; the Annual Orange Transparency Report on Freedom of Expression and Protecting Privacy, including both quantitative and qualitative information on responding to government demands; the annual vigilance plan; and non-financial reporting, including its universal registration document and integrated annual report. The transparency report was expanded during the reporting period, following an internal review process and assessor recommendation from the company's prior GNI asssesment. Risk assessments and progress in addressing risks, as well as controls and management of GNI issues, are described in the annual Vigilance Plan report and Universal Registration Document.

Orange discloses information on what personal information the company collects on different entity websites, through channels such as privacy policies, personal data protection policies, FAQs, and training materials. The company shares information about potential requirements for provision of information to government authorities through these channels as well.

In June 2021, Orange launched a new, outsourced, web-based, whistleblowing platform, "Hello Ethics." "Hello Ethics" is an international, centralized service, open 24/7 and accessible to both internal and external stakeholders, that ensures the protection of the whistleblower. It allows for the raising of serious abuses of human rights, with explicit references to "Infringement of privacy" and "abuse of freedom of expression." Depending on the category, reports are received either by the Chief Compliance Officer or the Manager in charge of the Vigilance Plan for review and action. Any stakeholder concerned by an actual infringement of privacy, human rights or environmental issues can **alert Orange anonymously**.

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 the assessors identified was the significant efforts the company undertook during this assessment period to integrate the GNI Principles into its Vigilance Plan, helping provide additional internal controls and structured oversight and engagement on risk management, even for local entities.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. There was continued discussion of some of Orange's processes for assessing GNI-related risks and the relationship with broader company risk management, as well as associated training. There was also discussion of how the company prioritizes its stakeholder engagement in terms of both issues and geographic focus.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessors reported on steps taken by Orange in response to recommendations from the third cycle, noting in particular improvements in the amount of information included in the company's Transparency Report, including case examples, as well as ways in which the new Vigilance Plan, its controls, and the Vigilance Plan Manager position have improved staffing and support for matters relevant to the GNI Principles and Guidelines and increased awareness of GNI-relevant issues across the company.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Merger & Acquisition Due Diligence -** The assessors made recommendations on how to strengthen review of human rights-related criteria in the company's non-financial M&A due diligence.
- **Service Restriction Demands -** The assessors complimented the company for having a policy specific to "major events" concerning freedom of expression and recommended that the policy could be broadened to include additional scenarios or supplemented with a Group-wide law enforcement assistance policy.

Telenor[17]

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

ABOUT THE COMPANY

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

WHOLLY OWNED	WHOLLY-OWNED – SUBSIDIARY	SHAREHOLDER
Telenor Norway	Telenor Denmark	Dtac, Thailand (minority)
	Telenor Sweden	DiGi, Malaysia (minority)
	DNA Finland	Grameenphone, Bangladesh (majority)
	Telenor Pakistan	
	Telenor Myanmar	

GOVERNANCE

Telenor's human rights commitment is anchored at the highest level through its governing documents, including the Telenor Code of Conduct, as well as a set of Group-level policies and manuals, processes and systems on monitoring and reporting, including the Authority Request Manual (AR Manual) and the Group Sustainability Policy, which are regularly reviewed and updated. Telenor's Board of Directors exercises oversight of the company's human rights practices with the support of its Sustainability and Compliance Committee (SCC) consisting of Board members. The SCC meets regularly for deep dives on issues including those related to the GNI scope, including ad hoc meetings for particularly challenging cases, and feeds this back to the Board. The Board of Directors also exercises oversight through its Risk and Audit Committee who receives direct reporting from the Head of Group Internal Audit. Group Executive Management, made up by heads of global units, serves as an advisory body to the CEO, also participating in deep dives on human rights issues.

17 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

Every group policy has a group policy owner and a local policy owner. The Group Chief People & Sustainability Officer owns the AR Manual and the Group Privacy Officer is the manager of the Manual. Local Boards and CEOs are accountable for the implementation of the AR Manual, with oversight from the local privacy lead. There are cross-functional teams, with experts from privacy, legal, sustainability and security, set up to address challenging authority requests at both the global and local levels. As necessary, requests are escalated to the Group Authority Request Steering Committee, which features several senior staff, in collaboration with the business unit CEO. Business units conduct human rights due diligence annually, which they report back to the Group.

The cross-functional Group Authority Request Team (GART) processes government requests, while Telenor's Group Sustainability team produces training material and conducts training sessions to ensure that all AR personnel have adequate integrity and legal, privacy, human rights, and technical competence to maintain confidentiality and to objectively assess whether a request shall be met, challenged, or escalated. In Q1 2020, Telenor Group launched a virtual Group-wide human rights training and in-depth human rights workshops targeting different key functions in each business unit. Business units provide additional targeted training for staff that are likely to be exposed to human rights issues. Telenor has established an internal site in December 2021 housing relevant material on HRDD, including the HRDD toolkit and e-learning.

DUE DILIGENCE AND RISK MANAGEMENT

Telenor employs an ongoing process of human rights due diligence to identify, prevent, mitigate and account for how to address human rights impacts, in alignment with the UNGPs. It is set out in the Group Policy Sustainability and is mandatory at both Group and BU levels. The HRDD toolkit stipulates that HRDD covers country context, industry context, company context, and the rightsholder and stakeholder context. BUs must conduct legal and human rights assessment upon receiving an authority request, and the AR Manual details that BUs must undergo regular reviews of country legal frameworks. Products must undergo a DPIA when access to data is involved, as set out in the Privacy Manual.

HRDD is embedded in Telenor processes that enable evaluation on a continuous basis, through the whole value chain. Telenor's human rights prioritization is based on the analysis of severity (scope, scale, and remediation) and management (likelihood, attribution, and leverage) of the risk(s) to identify salient issues. Issues that are seen to be of the highest priority are entered into each business unit's company risk register, and mitigation measures are regularly tracked. Telenor increases engagement with stakeholders where risks are identified. They also integrate human rights risk in the overall risk management approach, including for internal and supplier audits.

Respect for human rights and privacy are included in the Supplier Conduct Principles (SCP), which suppliers are legally obliged to comply with through the Agreement on Responsible Business Conduct (ABC)/SCP contract. The SCP includes privacy, freedom of expression and data protection issues. Telenor conducts regular reviews of SCP conformity and performance through annual self-assessment questionnaires and risk-based inspections programs. Audits are conducted as part of Telenor's participation in the Joint Audit Cooperation (JAC). Suppliers that handle personal data must also sign data processing agreements.

FREEDOM OF EXPRESSION AND PRIVACY IN PRACTICE

With regards to the handling authority directives, the GNI Principles are implemented through the AR Manual, which details that business units shall maintain an internal escalation process ensuring that the Data Protection Officer is involved regarding requests with unclear or doubtful legitimacy. The manual details a number of steps that the policy manager should take in responding to requests, including ensuring requests meet procedural and material requirements for a valid legal basis; requesting communications in writing with clear and complete requests; pushing back, to the extent possible, and/or

escalating requests where there are doubts if they may fail to adhere to procedure; and taking steps to ensure narrow interpretation to minimize impacts on users. The AR manual details additional mitigating measures:

- Regular reviews with relevant authorities of controversial authority requests, in order to seek clarification or modification;
- Regular judicial review (court-procedure) and/or appealing to other relevant branches of the administration, as available or controversial authority requests;
- Engaging in dialogues with relevant authorities to seek solutions that meet the authorities' needs with as little impact as possible;
- Engaging with stakeholders, such as other operators, industry peers, media and NGOs, as appropriate for support in the dialog with the authorities.

Business units are expected to engage with the authorities, in accordance with its Guidelines, and do so on a regular basis. Where possible Telenor also engages in consultations on upcoming laws and in international policy conversations, including through bodies like GNI. Telenor also engages local stakeholders directly (i.e. diplomatic community, CSOs, chamber of commerce) to provide a united front on challenges, enhancing multilateral advocacy where possible (accounting for the safety of local actors). This engagement benefits from reference to GNI statements. Group engages with the host government on a regular basis, often making references to GNI Principles.

Telenor has a company-wide Privacy Policy and Manual to minimize and mitigate the risk associated with processing personal data in all jurisdictions. Key principles include:

- Personal data should solely be used for the purposes for which the data was collected, and need to have a valid legal basis for processing.
- Each business unit has a privacy organization with responsibility for implementing the policy and manual, and a dedicated DPO.
- Each BU must conduct a data protection impact assessment of high-risk activities, have an inventory of processing, and have a procedure for ensuring data quality. Must implement technical and organizational measures to keep personal data secure.
- Telenor has a personal data breach manual detailing preventative requirements and requirements for responding should a breach occur.

TRANSPARENCY AND ENGAGEMENT

Telenor Group publishes an Annual Sustainability Report, as well as annual authority requests transparency reports, legal frameworks overview, and historic alignment reports with the GNI and the Industry Dialogue Principles. Both Group and BUs engage with shareholders and stakeholders through meetings and at events. As examples, Telenor's Director Human Rights participated in a plenary panel discussion at the UN Annual Forum on Business and Human Rights in November 2019 focused on responsible business in conflict affected areas, and the Group EVP provided a keynote at RightsCon in 2021.

Telenor discloses to users what personal information is collected through a privacy notice for each Telenor company, also in line with the GDPR. Telenor hosts a dedicated site, "handling legal requests from authorities" with information on relevant legal requirements, and shares country specific information on this site and in the GNI Country Legal Frameworks Resource. Telenor's annual Authority Requests Disclosure Reports provide legal overviews (also shared on the GNI Country Legal Frameworks Resource), information about policies and procedures, and indicates the number of requests received from authorities in each country in each of the categories (to the extent permitted under local law): communication data, lawful interception, network shutdowns, content restrictions and content distribution. When legally permitted, Telenor posts a notification, e.g. message on a landing page or a web post, detailing the company has received requests to restrict access to content or services, and Telenor may also share notice to the targets of investigations, subject to local law restrictions.

The global Integrity Hotline provides a channel to report concerns and ask questions about possible breaches of Telenor's Code of Conduct, including relevant laws, regulations, and Governing Documents. Queries and reports are handled confidentially and the individual using the hotline can choose to report anonymously. Employees can report suspected breaches of the Code of Conduct via the group compliance function.

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 assessor identified Telenor's efforts to engage through industry and multi-stakeholder initiatives as one of the main strengths and successes in implementing the GNI Principles. The assessor found that Telenor showed and explained their works with partners – both in public and privately – to find solutions together to vexing human rights quandaries.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. There was additional discussion of how the company can better track and report on government requests that may be objectionable, and requests that are escalated, but fail to meet normal standards and procedure and therefore are more difficult to categorize. There was also discussion on how the company is considering potential alignment between GNI commitments and emerging regulatory requirements for human rights risk assessment, reporting, and audit, including with experiences from the Norwegian Transparency Act.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessors reported on steps taken by Telenor to implement the recommendations received in the third cycle, including efforts to increase, better coordinate, and document training, strengthen oversight of supplier implementation of Telenor's Supplier Code of Conduct, and improve stakeholder engagement.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Integrating HRDD/HRIA Takeways -** The assessors recommended that Telenor consider ways to register key takeaways from HRDD and HRIA activities, including by integrating them into relevant, group-level policies.
- **Fostering Discussion -** The assessors recommended that Telenor consider ways to foster further discussion within GNI and with other stakeholders on the effect of European sanctions on freedom of expression and privacy in countries outside of the EU, as well as about responsible business conduct in and responsible exit from conflict-affected, high-risk contexts.

Telia Company[18]

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

ABOUT THE COMPANY

Telia Company provides the following products and servics:

- Mobile voice and data;
- Fixed voice and data
- TV and streaming
- Media advertising
- Value added services
- ICT services
- Devices

Telia Company's operations previously included Telia Carrier, the divestment of which was concluded June 2021.

Telia Company has its roots in Sweden and Finland. Today Telia Company operates in several Nordic and Baltic countries. During 2015, Telia Company announced the decision to reduce presence in the Eurasia region step by step, enabling full focus on the core markets. Telia completed its exit from Eurasia during the reporting period, divesting from minority ownership in Turkcell in October 2020 and completing divestment of operations in Moldova in March 2020. An **overview of Telia Company's geographic presence and business lines** is available on their website.

GOVERNANCE

Telia Company Group Policy on Freedom of Expression and Privacy provides the foundation for implementation of the GNI Principles. The Policy is owned by the Chief External Affairs, Governance, and Trust Officer, who is appointed on behalf of Group management. The Senior Advisor of Human and Digital Rights serves as the relevant internal subject matter expert, provides significant input on the design of Group policy, coordinates escalation procedures, and leads an internal human rights core team. Group Management members own specific group policies for issue areas of expertise, including responding to escalations. Telia Company's annual statement of materiality, owned by the Board, also references several international guidelines on human rights.

General Executive Management (GEM) meets regularly in the Group Governance Risks Ethics and Compliance forum (GREC), which acts as a governing body for risk management and compliance. Additional GRECs are established on Group and country level or where Group GREC assesses it to be needed. Group GREC also reports to the Audit Committee of the Board, which exercises additional oversight, receiving internal and external audit reports and information about GNI assessments.

18 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

Each Group Executive reporting to the CEO of Telia Company is responsible for ensuring that the Policy is duly communicated and implemented, and that the employees within his/her area of responsibility are familiar with and follow the Policy. Hands -on guidance is provided in relevant instruction and a form for escalations. Since Q2 2021, all employees have access to a training about human rights in the internal site for online training. The Company Code of Responsible Business Conduct training, mandatory for all employees, includes a chapter on freedom of expression.

DUE DILIGENCE AND RISK MANAGEMENT

When adopting the new company purpose and strategy in Q1 of 2021, Telia Company integrated sustainability, including freedom of expression and surveillance privacy, into the company strategy. This approach was informed by a sustainability materiality assessment (see page 49 of the 2020 materiality report), as well as an exercise led by the Group Human Rights Core Team to define salient human issues in Telia's impact areas (see page 54 of the 2020 annual and sustainability report).

An enterprise risk management (ERM) process, adopted in Q2 2021, where each defined risk priority area is owned by an appointed member of Group Management, includes freedom of expression and privacy as priority risk areas, and provides a systematic assessment of risk levels and associated controls. The ERM is designed to revisit issues over time, and the Board receives risk reports based on the outcome twice a year. Telia Company's policy on freedom of expression and surveillance privacy also includes a 'bottom-up' escalation procedure for potentially high-risk (unconventional) government requests. Such escalations surface issues for analysis, mitigation, and prevention on an ongoing basis. Mitigation activities are approved by the Group General Counsel.

During the reporting period, Telia Company started implementing privacy by design in all products and services. A data protection impact assessment is conducted before carrying out any data processing that is likely to result in a high risk to the rights and freedoms of users.

Telia Company's human rights due diligence work is guided by the UNGPs. Topics for HRIAs may be raised by Group GREC, as part of continuous work of the sustainability team (including the core human rights team), by local and functional GRECs, or as part of escalations. Outcomes of HRIA are brought to relevant countries/functions for knowledge building and to enable changes in policies or processes if needed. HRIAs have been conducted for a wide range of scenarios, including market exit. Telia's supplier code of conduct includes human rights requirements and additional guidance for suppliers to respect the rights to privacy and freedom of expression.

FREEDOM OF EXPRESSION AND PRIVACY

The Telia Company Group Policy on Freedom of Expression & Surveillance Privacy describes how the company will assess and respond to government requests and demands with potential serious impacts on freedom of expression and privacy. In addition to the publicly available policy, the corresponding Group instruction on freedom of expression and privacy sets out how the policy is implemented. This includes requiring governments to follow established domestic legal processes, requesting clear written communications, and soliciting the narrow interpretation of government requests. The form for assessments and escalations provides additional hands-on guidance for potential unconventional requests. The Group instruction, in sum, sets out the following objectives:

- Respect, promote and advance the freedom of expression and privacy of individuals;
- Assess and escalate requests and demands from governments and authorities that might have
- potentially serious impacts on freedom of expression and privacy;
- Document and log unconventional requests or demands, and related company actions; and
- Act transparently, as far as possible, vis-à-vis external stakeholders.

If in doubt, the Group policy states to always treat requests or demands as potentially having serious impacts on freedom of expression and surveillance privacy. The Group Instruction details that requests received outside of the local company's normal routines, such as directly by a Group function or other unit or person and/or when the accredited personnel handling requests and demands is outsourced, should immediately be escalated. For lawful intercept requests, Telia Company has set up local internal processes for interaction with the authorities to handle each single interaction.

In addition to the escalation procedure described above, Telia Company has set up a whistle-blowing tool, the Speak-Up Line available at https://secure.ethicspoint.eu/domain/media/en/gui/101615/index.html,

to provide a secure channel through which employees, as well as external stakeholders, can confidentially or anonymously report human rights issues and violations, including the Group Policy.

The Group Policy and corresponding instruction identify "significant changes or proposed changes in the law, or significant imposed or proposed operational changes, in the context of freedom of expression and surveillance privacy" as examples of unconventional requests. Telia Company advocates for clear and transparent legal provisions on proportionality and necessity for all government surveillance of communications, and argues that government surveillance should be conducted under the supervision of a court or other independent judicial body. The company regularly comments on legislative proposals, participates in industry organizations locally and internationally, and undertakes regular reporting, including on unconventional requests, to inform policy debates and provide transparency (more below).

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.

Some key tools for communicating the company's approach include:

- Statement of Materiality
- Code of Responsible Business Conduct
- Human Rights Policy, with context
- Policy on Freedom of Expression and Surveillance Privacy, with context
- Articles on major events in the context of freedom of expression and surveillance privacy
- Formal public reporting
- **Annual and Sustainability Reporting**
- **Law Enforcement Disclosure Reporting**

The group instructions include provisions on transparency, such as publishing information on unconventional requests and company responses, when not prohibited under law, and working to raise awareness on relevant legal frameworks. The company also commits to provide clear, prominent, timely notice to users when access is blocked or communications have been limited or stopped due to government restrictions, sharing the reason for the restriction, and identifying the relevant authority where legally possible.

Telia Company has Privacy Policies applicable for its different companies, products, and services that contain information about what personal data we process and how, in accordance with the EU GDPR's transparency obligations. The Privacy Policies are provided to Telia's customers at the time of onboarding and are publicly available on the website.

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 assessors observed that Telia has strengthened overall sustainability governance and reporting processes related to e.g., the Board, GEM, and GREC. This included significant attention from local and Group management in responding to unconventional requests. The assessors took note of the company's progress with undertaking risk assessment of products, including implementing privacy by design, while recommending the company consider implementing similar formalized processes for potential freedom of expression risks.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. There was discussion around Telia's good practices for human rights due diligence and impact assessments around market entry and exit, as well as potential contractual mitigations and other due diligence after sale. There were also discussions about avenues for additional transparency for national security-related requests, as well as the challenges brought forth by **direct access** regimes. There was also discussion of how GNI materials can be helpful for both internal and external awareness raising on freedom of expression and privacy.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessor reported on Telia's efforts to implement previous recommendations, including efforts to clarify relevant roles, formalize and strengthen escalation and reporting processes, and implement privacy-by-design for all products and services.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Training on Relevant Issues -** After noting the importance of existing trainings that incorporate freedom of expression and privacy, the assessors recommended that Telia implement formal training specifically on freedom of expression and privacy-related issues for relevant employees.
- **Third Party Due Diligence -** The assessors recommended that Telia build on its existing supplier-focused efforts to enhance human rights due diligence in connection with other, non-supplier, third parties.

Vodafone[19]

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

ABOUT THE COMPANY

Vodafone Group Plc is a multinational telecommunications company, registered in the UK. Vodafone is the largest pan-European and African telecoms company with a purpose to connect for a better future by using technology to improve lives, digitalise critical sectors and enable inclusive and sustainable societies.

As at 31 March 2021, Vodafone provided mobile and fixed services in 21 countries, partners with mobile networks in 49 more. Together, Vodafone serves over 300 million mobile customers, more than 28 million fixed broadband customers, over 22 million TV customers, and more than 123 million IoT devices. Vodafone Group provided services to 19 Operating Companies (OpCos) and 2 Associates/Joint Ventures in the following countries:

- Europe: Albania, Czech Republic, Germany, Greece, Hungary, Ireland, Italy, the Netherlands (joint venture), Portugal, Romania, Spain and the United Kingdom.
- Africa: the Democratic Republic of the Congo, Egypt, Ghana, Kenya (associates), Lesotho, Mozambique, South Africa, and Tanzania
- Other Markets: Turkey.

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, which range from small businesses to large multinational companies.

More information on Vodafone Group's geographic footprint is available on **its website**.

GOVERNANCE

The Vodafone Group External Affairs Director is the most senior company representative with responsibility for human rights, including the GNI Principles. The Group External Affairs Director is a member of the Vodafone Group Executive Committee ("Group Exco"), which is responsible for strategic oversight of the Group's human rights policies through various mechanisms, including sponsorship of policies, relevant reports on human rights issues, use of subcommittees and other groups as part of overall company due diligence and governance activities integrating freedom of expression and privacy, consultation and sign off on external stakeholder engagement and GNI engagement. Responsible subcommittees and other groups with representatives from executives and senior management include the Audit and Risk Committees, the Human Rights Advisory Group, the Risk and Compliance Committees, the Policy and Reputation Steering Committee and the ESG Committee.

19 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

Within senior management the Sustainable Business team has lead responsibility for the implementation of the GNI Principles with other senior management teams, including Security, Privacy and Policy. These teams work closely with their OpCo counterparts on sensitive FoE and privacy related issues. The GNI Principles are integrated into routine business operations, through Group policies and implementation guidelines, risk identification and mitigation processes, including escalation processes, product development and design, governance, contractual structures, ongoing monitoring, and reporting and transparency. All employees, including Group Exco, senior management and frontline personnel, undertake Code of Conduct and 'Doing What's Right' training, which includes coverage of freedom of expression and privacy risks, and additional, targeted training is provided for relevant personnel.

Vodafone Group's policies apply to all Vodafone companies in which Vodafone Group holds an interest of 50.1%, or more, or management control. Where it has less control, it operates a Related Entity framework, which includes Vodafone Group's minimum expectations, including respect for human rights.

DUE DILIGENCE AND RISK MANAGEMENT

Vodafone Group's approach is to embed a human rights impact assessment into the due diligence process in a number of operational scenarios. Where higher risks to rights are identified by the Human Rights Senior Manager, whether due to scale of impact, scope or likelihood of remediation, a more detailed risk assessment is conducted and is escalated.

As detailed in Vodafone Group's Human Rights Policy Statement, this could include scenarios when developing new products/services/ technologies or making substantial changes to existing offers; entering new countries or in anticipation of changes in existing operating environments; considering new partnerships/ acquisitions; and engaging with suppliers.

Vodafone Group Corporate Security, in parallel with Cyber Security and Privacy, operates a Security and Privacy by Design Programme ("SPDA"), which ensures all new products and services developed within Vodafone Group are reviewed and developed in line with Vodafone Group policy and local security and legal obligations. Any activity by Vodafone Group which involves personal data processing must go through a Privacy Impact Assessment, irrespective of whether it is a product or service launched externally.

All potential business relationships undergo due diligence as part of the overall company governance. For new partner markets, an analysis is conducted of both the country and prospective partner in question by the Risk and Intelligence team within Group External Affairs, which is then reviewed by the Human Rights Senior Manager. Actions as a result might include a decision not to go ahead, or a decision to go ahead but with appropriate safeguards specific to that country or through policy control frameworks.

Vodafone Group keeps track of changes relevant to policies using a digital strategic risk register providing 'line of sight' reporting on current risk issues. Details of risk issues are uploaded and this allows them to be monitored and reviewed, on that platform, on an on-going basis. It also enables functionality which allows the business to set tailored time scales for revisiting issues and reviewing progress in managing and mitigating risks.

In relation to business partners, Vodafone Group uses its leverage through being clear on its expectations, through policies such as the Vodafone Group Code of Conduct and Business Principles, which apply to everyone working for or on behalf of Vodafone group; its Ethical Purchasing Code; the Acceptable Use Policies and contractual clauses which include specific reference to risk to human rights.

FREEDOM OF EXPRESSION AND PRIVACY

Vodafone Group Law Enforcement Assistance (LEA) policy outlines the governance and safeguards Vodafone Group has in place to ensure it appropriately balances respect for its customers' right to privacy and freedom

of expression with its legal obligations, to support a free and secure society. This policy must be adhered to by employees, contractors, suppliers, and directors. The LEA policy is owned by the Group External Affairs Director and championed by the Group Corporate Security Director. The Senior Manager, Legal Interception and LEA support is responsible for day to day implementation of the policy. Due to the Vodafone Group and operating company structure and national security requirements, individual OpCos have responsibility for the implementation of the LEA policy within the legal jurisdictions in which they operate.

Vodafone Group has a set of detailed requirements to outline the process that should be followed when an LEA support request is received. The detailed requirements include a breakdown of five key stages when handling a Government demand. The Vodafone Group Human Rights Policy also includes a specific section on escalations for certain law enforcement requests that may infringe upon privacy and freedom of expression.

During the reporting period, Vodafone Group implemented three new policy and assurance controls related to the LEA operations to further embed the policy in OpCos, including training, reporting and legal assurance. These additional controls aim to give further transparency and assurance to the Vodafone Board as well as ensuring relevant escalations, if required, are made on a timely basis. The LEA policy is reviewed on an annual basis to ensure that it is 'fit for purpose' and periodic testing is undertaken and reported on.

In addition to the LEA policy, the internal 'Safe and Secure Toolkit' provides specific advice and guidance to Group entities and its local markets on engaging with new proposals (such as new legislative proposals or requests for capability) from governments, and Vodafone Group's Freedom of Expression Principles call upon government to follow international law and standards. Consultation and engagement with governments is done by both local entities and centrally by group teams.

The **Vodafone Group Privacy Centre** explains how Vodafone Group's privacy policies and framework govern how the company collects, uses and manages customers' information in order to ensure the company respects the confidentiality of their personal communications and any choices that they have made regarding the use of their data. The protection of personal data is one of Vodafone Group's highest priorities and is central to the Vodafone Group Code of Conduct.

TRANSPARENCY AND ENGAGEMENT

Vodafone Group publicly reports its human rights impacts in relation to privacy and FoE in a number of ways including, for example, on the **Vodafone Sustainable Business website**. The website includes information on Vodafone Group's approach to human rights, law enforcement assistance information, and its approach to ethical sourcing, amongst other materials. In 2021, Vodafone Group changed the process and mechanism for sharing and providing its transparency reporting relating to Law Enforcement Assistance demands. This included new pages to explain the following areas:

- Handling Government demands;
- Challenges for operators;
- Managing government demands;
- Our principles and policies; and,
- Government Assistance demands reporting.

FoE 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 internal teams. Privacy specific queries can also be submitted to the **dedicated site** for specific local entities.

More general enquiries on freedom of expression, privacy and human rights from external stakeholders are also often made through the media enquiry lines or directly to relevant individuals within the Vodafone Group Sustainability Team.

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 assessor expressed appreciation for the companies' progress in centralizing its GNI commitments with senior-level oversight during the reporting period, and recognized that integration of GNI principles was visible throughout the company. The assessor noted that it remains important to continue to further review and ensure that sufficient resources devoted to human rights expertise in the company. In addition to personnel, the assessor found that Vodafone Group also cleverly utilizes technology and existing compliance systems to ensure human rights issues are part of everyday company procedures and processes, including in local markets.

During the Board Review Meeting, which featured representatives from GNI's multistakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. One topic was the companies' ability and efforts to influence the practices of partner markets or other business relationships where the company may lack operational control, including steps the company takes in contractual mitigations. Another topic discussed was scope of the company's ability and approach to providing notice to users in response to government-ordered content restriction and service disruption, considering both potential legal restrictions and measures for greater disclosure where possible.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessors reported on Vodafone's efforts to implement recommendations from the previous assessment cycle, including steps to increase the training around freedom of expression and privacy, embed standardized human rights assessment questions into relevant processes, and introduction of new controls to monitor compliance with the LEA policy across the company.

Yahoo[20]

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

ABOUT THE COMPANY

Yahoo is a media and technology company with a global presence. Yahoo offers mail services through Yahoo mail and AOL mail as well as original and curated editorial content through Yahoo News, Yahoo Sports, Yahoo Finance, TechCrunch, and Engadget. Yahoo's products have changed over the last five years, with a shift away from services featuring user-generated content. This includes the sunsetting of Yahoo Answers (2021) and Yahoo Groups (2020), and the sale of Tumblr (2019) and Flickr (2018). In 2021 Verizon sold Verizon Media (now known as Yahoo) to funds managed by affiliates of Apollo Global Management. Yahoo now operates as a standalone company under Apollo Funds. The sale of Yahoo took place at the end of this assessment cycle.

GOVERNANCE

Yahoo has adopted a company-wide commitment to operate with respect for human rights in line with the Universal Declaration of Human Rights. Yahoo's Business & Human Rights Program (BHRP) is responsible for providing leadership on global strategy, business decision-making, and internal and external engagement on human rights matters, including driving the implementation of the GNI Principles. The BHRP is led by the VP for Global Public Policy and is overseen by the Chief Legal Officer. Senior executives in the company, including members of the Board of Directors, receive briefings by the BHRP. The BHRP works cross-functionally and collaborates with multiple teams across the organization. The BHRP regularly conducts internal training, in-depth consultations, and information sharing sessions with employees and teams on Yahoo's human rights commitments, including the GNI Principles. Following the sale of Yahoo in September 2021, the BHRP delivered briefings on the GNI Principles to the Legal Department, which included the leads for privacy, law enforcement, ethics & compliance, trust & safety, international legal affairs, legal transactions, and global public policy.

DUE DILIGENCE AND RISK MANAGEMENT

The BHRP works to drive responsible decision-making and integrate a focus on human rights issues, including privacy and free expression, in business decision-making processes across the organization. To do this, the BHRP team identifies potential human rights risks and opportunities that could arise from Yahoo's products and operations and makes recommendations to avoid or mitigate those risks. As part of this, the BHRP provides analysis and strategic advice before final clearance for a range of decisions that have human rights implications such as those related to product launches, modifications, decommissions or changes to legal structure, entry into a new geography, acquisitions or dispositions, partnerships or divestment.

20 This section is a summary of certain information that was reviewed and presented in the company's GNI assessment report, which reflects the company's business, structure, and policies at the time of assessment (2021). It has not been updated to incorporate changes that may have occurred since then.

yahoo!

The BHRP also participates in product reviews and launch processes and provides inputs into the high-risk partnership and deal review process.

The BHRP is responsible for performing ongoing human rights due diligence on Yahoo's business decisions. This includes undertaking both short-form and long-form human rights impact assessments (HRIA's) on decisions related to Yahoo's operations, products, or services. Yahoo prioritizes human rights issues raised through its human rights due diligence process according to the salience of the issues, the likelihood and severity of risk, the jurisdiction in question – including the local law, government human rights practices, and safety of local employees – and based upon the level of control Yahoo has to prevent, mitigate, or remedy the harm identified, consistent with the GNI Principles and the UNGPs. There are a number of circumstances that may trigger a decision to conduct an HRIA. Some examples include entry into new geographies, significant legal or political changes in geographies where Yahoo already does business, launch of new or updated products or services, and development or use of relevant automated systems, such as content moderation systems, that may impact the rights of users. Long-form HRIA's undertaken by the company are also informed by external stakeholder input and after an HRIA is completed, and as appropriate, Yahoo will reach out to external stakeholders to inform them of the decisions made.

The BHRP establishes paths for escalating human rights related issues to the Chief Legal Office or other leaders as needed. There are also internal channels through which personnel can discuss or raise issues or concerns related to Yahoo's GNI commitments including through the company's ethics reporting system. The Yahoo Ethics & Compliance site is available to the public to report potential issues related to the human rights impacts of Yahoo's activities or to ask questions about the company's human rights commitments.

PRIVACY AND FREEDOM OF EXPRESSION IN PRACTICE

Yahoo's Global Principles for Responding to Government Requests are informed by the GNI Principles and outline how Yahoo will respond to government requests for access to data and removal of content. Yahoo's Law Enforcement Response Team is responsible for implementing the Principles, which commit the company to:

- **Minimize disclosure of user data and restrictions to freedom of expression online.** We minimize the disclosure of user data and the restriction of user content by narrowly interpreting government requests in these areas.
- **Protect human rights, including the rights to privacy and freedom of expression.** We examine all appropriate options when faced with a government request that raises human rights concerns, including seeking clarification or modification or contesting the request.
- **Be accountable and transparent with our users.** We share information with our users about how we handle government requests and about our disclosure of user data and removal of content.

With respect to privacy, the Yahoo Privacy Policy, developed with input from the BHRP, details what types of information the company may collect, how data is stored, and for what purposes the data is used. Yahoo has also developed a micro site that provides information as to how and when user data is collected and used. A privacy dashboard allows users more granular control over how and when their data is used. Users can also learn more information about what laws govern their account through the Yahoo Terms of Service.

In accordance with the GNI Principles, Yahoo commits to interpret government requests for access to user data narrowly and produces the least amount of data necessary to respond to lawful orders. Yahoo commits to only disclosing user data in response to a valid legal process or in appropriately stated emergency situations. If a request

yahoo!

has not been made in accordance with these requirements, Yahoo will push back on the request. As outlined in the Yahoo Privacy Policy, Yahoo commits to notifying users about third-party requests for their information prior to disclosure, unless prohibited from doing so by law.

With respect to freedom of expression, Yahoo's Global Principles for Responding to Government Requests, Terms of Service, and Community Guidelines guide the company's response to government requests for content removal. Yahoo also takes into consideration applicable law and international human rights laws and standards in making decisions related to content. The Trust & Safety team at the company is responsible for reviewing all requests for removal of content. The team applies the same policies, processes, and standards to content related decisions regardless of whether content is reported by governments or users. Requests from governments may be further reviewed by the Law Enforcement Response Team with guidance from the BHRP. When a user's content is removed or blocked, Yahoo may notify users via email. By following the link provided within the notice, or contacting Yahoo through the Help Page, users can request that Yahoo review its decision related to a piece of content. Each appeal is reviewed by a member of Yahoo's support team. Yahoo also works with a third-party to moderate comments on Yahoo News articles according to Yahoo's Community Guidelines and Terms of Service.

TRANSPARENCY AND ENGAGEMENT

Yahoo's commitments to the GNI Principles are discussed on the BHRP website, which is part of the corporate website and its Transparency Reporting Hub. Through the Transparency Reporting Hub, Yahoo regularly reports on the number of requests for user data and content removal the company receives from governments as well as the company's response rates. The Transparency Reporting Hub also hosts information about applicable laws and policies which require the company to restrict content or communications or to provide personal information to government authorities, as well as the types of legal requests Yahoo may receive and what type of data may be disclosed in response to each type of legal request.

Yahoo also undertakes engagement with different organizations and stakeholders. The Yahoo Global Public Policy team engages with organizations and processes to encourage governments to respect users' rights. In addition to participation in GNI, examples include participation in the Reform Government Surveillance coalition, lobbying against governmental reforms that would limit Yahoo's ability to serve content in a country, and working with other tech companies to oppose expansion of state surveillance laws.

FOLLOW UP AND IMPROVEMENT

During the assessment meeting, 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 assessor identified Yahoo's commitment and work to ensure the continued implementation of the GNI Principles during times of significant organizational change as one of the main strengths and successes in implementing the GNI principles. This included maintaining robust HRDD practices amid significant changes to the business, as well as continued commitments from leadership and continuity in policies.

During the Board Review Meeting, which featured representatives from GNI's multi-stakeholder Board, the company, and the assessor, additional strengths and challenges were discussed. This included discussion on the company's approach to HRDD and HRIAs, the BHRP's evolution, and resourcing for the BHRP given changes in the company. There was also discussion with the company on various themes, including government demands for providers of journalistic content, considerations about identifying users that are targets of sensitive data requests, and questions of jurisdiction.

yahoo!

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative. Further examples and trends drawn from across the recommendations can be found below in the **Improvement Over Time section**.

RECOMMENDATIONS FROM THE THIRD GNI ASSESSMENT CYCLE:

The assessors noted steps that had been taken to expand internal education and training, as well as to facilitate knowledge sharing across LERT teams within Yahoo, consistent with recommendations made in the prior cycle.

RECOMMENDATIONS FROM THE FOURTH GNI ASSESSMENT CYCLE:

- **Navigating Change -** While remarking on the resilience of Yahoo's human rights commitments and policies, the assessors noted the significant changes that were taking place at Yahoo during the assessment period and emphasized the importance of prioritizing continuity amidst these developments.

5.

Improvement Over Time

5. Improvement Over Time

To enable companies to continue to improve and evolve their policies and practices, the GNI assessment uses the standard of "good-faith efforts to implement the GNI Principles with improvement over time." Measuring improvement overtime allows for an assessment of how companies are improving their practices to better protect privacy and freedom of expression in response to evolving challenges and threats in the digital landscape. A key part of the assessment process are the non-binding recommendations that can come from assessors and the GNI Board, which are meant to provide the company guidance for considering changes to their policies and processes to better implement the GNI Principles.

Companies may choose to implement a recommendation, reject it, or take different steps to address the core issue in the recommendation. If a company addresses the issue in a recommendation another way or rejects a recommendation, it will explain its decision to the GNI Board in its next assessment. 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. During the assessment meeting, the GNI Board considers steps taken pursuant to prior recommendations in the context of its determination. As noted in the Assessment Toolkit, individual Board members may also provide informal feedback during the assessment review meeting.

RECOMMENDATIONS FROM ASSESSORS

During the 2023 assessment cycle, assessors made a total of 66 recommendations to the 11 assessed companies. Recommendations given by assessors centered around the four main categories from the Assessment Toolkit: due diligence and risk management; freedom of expression and privacy in practice; governance; and transparency and engagement. This section outlines key trends that emerged across recommendations from assessors. These are consistent with and in many ways reflective of the company-specific recommendations set out in the **Company Determinations section**.

DUE DILIGENCE AND RISK MANAGEMENT

Risk Management: Across companies, assessors highlighted ways in which companies could strengthen the structure, content, implementation, oversight, and documentation of policies and processes related to identifying emerging risks. This included through steps such as regular engagement with local stakeholders, ensuring that relevant procedures and/or manuals include appropriate human rights triggers, and ensuring new products are assessed for risks to both privacy and freedom of expression. There was a focus on ways to apply risk management processes to high risk markets and during crisis situations. Examples of suggested steps companies can take when navigating such situations include: deepening internal capacity around international humanitarian law, putting frameworks and appropriate escalation channels in place to proactively assess local contexts, and ensuring the consistent application of due diligence procedures when responding to government requests during crisis situations.

BREAKDOWN OF RECOMMENDATIONS IN THE 4TH ASSESSMENT CYCLE

ASPECT OF ASSESSMENT	NUMBER OF RECOMMENDATIONS
DUE DILIGENCE AND RISK MANAGEMENT	12
Risk Management	5
Due Diligence	4
Human Rights Impact Assessments	2
Other Business Relationships	1
FREEDOM OF EXPRESSION AND PRIVACY IN PRACTICE	13
Policies and Procedures	12
Other	1
GOVERNANCE	24
Board Oversight	4
Escalation	2
Internal Structures	10
Training	6
Senior Management	2
TRANSPARENCY AND ENGAGEMENT	17
Engagement with Governments	2
Engagement with Rightsholders	1
Transparency Reporting	2
Internal Communications	3
Other	9

Due Diligence: Recommendations emphasized the importance of companies having in place processes for documenting and 'auditing' past HRDD decisions in order to: ensure that processes are being implemented correctly; understand their effectiveness (particularly when applied at scale); and identify points of improvement. The importance of ensuring relevant policies and processes are formalized and applied to merger and acquisition activities was also highlighted. This included implementing due diligence processes across third party relationships a company may enter into and monitoring mitigation steps placed in contracts after products have been sold.

Human Rights Impact Assessments: A need for companies to further formalize processes and policies for the implementation of HRIA's was underscored. Suggested ways in which this could be done included developing formal processes for documenting institutional knowledge and memory, consistently following documented methodologies for HRIA's, mapping and retaining adequate documentation around decisions and actions undertaken during an HRIA, and improving transparency around the conduct and outcomes of HRIAs. In particular, the importance of thorough documentation of due diligence policies, processes, and decisions by human rights teams was stressed as key to preserving institutional memory and making sure that human rights processes and policies do not become siloed in a single department or individual.

FREEDOM OF EXPRESSION AND PRIVACY IN PRACTICE

Policies and Procedures: Recommendations highlighted ways in which policies and procedures related to freedom of expression and privacy could be improved. This could include ensuring that the application of relevant policies is comprehensive and consistent - extending across all the platforms, services, and products of a company. Company policies could also, to the extent possible, clarify different legal constraints local entities might be operating with. For example, it was recommended that company policies should recognize and seek to address situations where a local entity is unable, under local law, to inform its parent company of a government demand. Recommendations also noted that, to the extent possible, companies should ensure that data subjects are notified of government requests for user information and interpret these requests as narrowly as possible. Specific suggestions as to how companies could narrowly interpret requests included asking government authorities to clarify details/location of the data they are requesting and providing sufficient guidance to employees on what might constitute information which adversely affects or identifies another person and what to do in such situations.

GOVERNANCE

Board Oversight: Across companies, assessors emphasized that boards should be regularly briefed with sufficient detail on the implementation of the GNI Principles to provide strategic oversight and remain accountable for the same. In particular, boards should continue to receive detailed briefings even if responsibility for addressing freedom of expression and privacy risks has been assigned to sub-committees, a practice that was seen in multiple companies.

Internal Structures and Resources: The importance of companies having the policies, processes, resources, and capacity to manage governmental requests and undertake due diligence at a global level was a key trend that emerged in recommendations. This included growing the capacity of relevant teams to undertake regional engagement, developing tools to scale work, and developing the structures to respond to crises.

Training: The need for companies to invest in further training of personnel on human rights policies, the GNI Principles, and related processes at every level was highlighted across recommendations. For example, recommendations noted that to be effective, training should clarify how a role intersects with the implementation of the GNI Principles. Organizational mappings of job positions that may touch on issues relevant to the GNI Principles could help ensure that employees facing these issues receive the training they need. Recommendations also underscored the importance of ensuring continuity in human rights policies and processes as companies undergo internal changes to protect against the loss of institutional knowledge and cultural commitment.

TRANSPARENCY AND ENGAGEMENT

Engagement with Governments: When engaging with governments, recommendations noted the importance of companies explicitly referencing GNI and the GNI Principles in order to support their responses and continue to raise awareness of the GNI Principles and the organization's related work.

Engagement with NGOs: The importance of engaging with local stakeholders to identify risks and understand the effectiveness of measures taken was consistently pointed to across recommendations. Examples of practices related to engaging with NGOs included adequate and transparent documentation of engagement, allocating resources for stakeholder engagement, and developing pragmatic approaches to engagement at a global scale.

Transparency Reporting: As explained in the Company Determinations, all GNI companies engage in transparency reporting and many have developed pioneering approaches to enhancing public awareness of government demands. This cycle there were additional recommendations on how reporting on government demands could become even more granular and informative, as well as the importance of ensuring that the transparency reports of diversified companies include information related to their various platforms, services, and products.

External Communications: Across companies, assessors noted an increase in positive actions taken by companies in relation to human rights. Yet, information about these actions is often not communicated or communicated effectively to the public and other key stakeholders including shareholders. Recommendations underscored the importance of clear messaging from executive level leadership with respect to a company's commitments to human rights. Other suggested avenues to improve external communication of human rights commitments included annual human rights reports, media statements, blog posts, and meetings with stakeholders. Where possible, companies should also consider publishing information on HRIA's to the public or a select group of stakeholders.

> In our collective pursuit of a more responsible and rights-respecting digital landscape, we find valuable support in the GNI's Assessment Toolkit and Implementation Guidelines. The unique aspect of this assessment process is characterized by a standard of good-faith efforts. It's worth noting that human rights organisations are involved in this process of corporate accountability, which in the face of government demands and restrictions, is a significant measure to guarantee those rights for everyone.
>
> JUAN CARLOS LARA, Derechos Digitales

RECOMMENDATIONS FROM THE BOARD

During the assessment meeting, the GNI Board may also make recommendations to a company on ways to improve the implementation of the GNI Principles. Board recommendations are approved by a majority vote. During this assessment cycle, the GNI Board made a total of 6 recommendations. Examples of the focus of these recommendations include:

- Ensuring human rights teams have adequate resourcing and training to operate at a global scale and in multiple markets.
- Finding ways to improve and scale stakeholder engagement across contexts where a company operates
- Increasing the availability and implementation of company policies and practices across multiple languages

UPDATES ON RECOMMENDATIONS MADE IN THE THIRD ASSESSMENT CYCLE

The assessment reviews conducted in this fourth cycle, included updates from companies and assessors on steps taken pursuant to recommendations made in the prior (third) cycle. While these recommendations broadly fall into the same categories identified above, some notable points that came up regarding steps taken by companies to implement recommendations across these cycles include:

- Creation and expansion of senior positions and/or teams within companies responsible for human rights programmes and policies.
- Increasing the amount and types of training on human rights available to employees across the organizations and facilitating greater information sharing on human rights issues across departments and teams.
- Further formalizing and strengthening policies related to the implementation of the GNI principles. Examples included clarifying roles, strengthening escalation processes, embedding standardized human rights assessment questions into relevant processes, and introducing new controls to monitor compliance with company policies.
- Sharing more information in transparency reports and complementing it with context and explanation.
- Improving approaches to stakeholder engagement, including through more frequent engagements on a broader range of issues.

The fact that recommendations from this assessment cycle also focus on similar themes from previous cycles demonstrates how improvement within a company is an ongoing and iterative process that can continuously be improved.

RECOMMENDATIONS TO GNI

GNI, like its members, is committed to improvement over time. As such, the Assessment Toolkit includes a question asking assessors to provide specific recommendations they may have on how GNI may be able to improve its independent assessment process. This section summarizes assessor recommendations to GNI during this fourth assessment cycle.

IMPROVEMENTS TO THE PROCESS REVIEW

- Consider following a full audit process cycle with one or two cycles where there is more restricted assessment of progress against recommendations coming out of the full GNI audit cycle.
- Consider a calibrated approach in assessing how organizations are implementing GNI Principles. For example, GNI could seek to understand how a company is adapting to changes within particular countries or with regard to identified technologies.

IMPROVEMENTS TO THE ASSESSMENT TOOLKIT

- Continue to clarify how the GNI principles apply to vendors and indirect involvement in handling government requests.
- Consider benchmarking with other international human rights standards, current regulations, and emerging human rights and environmental due diligence laws.
- Consider crafting sector-specific assessment protocols to allow for a more nuanced assessment of participants in different industry groups.

IMPROVEMENT TO CASE STUDIES

- To increase the variety of GNI Principles covered by the case studies and provide additional options to the company and the assessors, the Case Selection Working Group could include up to four case studies for review in future assessments. These additional case studies would ensure that the focus of the assessment is consistent with themes or questions that non-company stakeholders want to address and would further guide the assessment.

6.

Challenges and Opportunities

6. Challenges and Opportunities

What might the world look like if GNI had never been born 15-years-ago, or if it had not flourished and expanded in the time since? While this sort of speculation can be ahistorical, the consistent progress and alignment over time of policies, processes, systems, and approaches of so many different companies, as demonstrated in this report, provides evidence that ICT companies, with support from and in collaboration with non-company actors, continue to provide a critical bulwark against government overreach.

But the assessments also tell a darker story, pointing out how geopolitical tensions, disrespect for rule of law norms, enhanced government pressure on the tech sector, and deteriorating civic space are combining to make it increasingly difficult for companies and civil society alike to hold the line. This section outlines some of the broad challenges GNI companies are facing as they seek to implement the GNI Principles, as well as the kinds of innovation, collaboration, and foresight that will be needed order to mitigate, and ultimately reverse, these trends.

CHALLENGES

One constant theme over the course of four GNI assessment cycles, is the continuous evolution and expansion of government efforts to conduct surveillance and manipulate the information space. Fifteen years ago, most governments had little or no clear authority to make demands for user data or censorship, especially regarding Internet-enabled services. Since then, and in no small part in response to push back by GNI members, many governments have enhanced their authorities and developed less direct, more "creative" ways to achieve similar ends. The chart on the next two pages provides a taxonomy of the various ways that governments seek to access user information and/or restrict expression, as illustrated through GNI assessments.

Complicating matters further for companies is the fact that governments are experimenting with this expanded toolkit at a time when global geopolitical developments are emboldening authoritarian and autocratic governments, while simultaneously leading some democratic governments to pull their punches and shy away from visibly defending companies or confronting those who make inappropriate demands of them. This most recent cycle of assessments illustrates vividly how companies' ability to resist or mitigate the impact of overbroad government demands or restrictions is especially limited in the context of conflict scenarios, public emergencies, and elections.

As illustrated in a number of assessments and case studies from this cycle, one reasonable outcome of risk assessment and responsible company decision making in these challenging contexts is to avoid entering or consider exiting certain challenging jurisdictions. But if responsible tech companies avoid these contexts, users are left even more vulnerable. These scenarios have provoked discussions within GNI and beyond about what responsible entry, remain, and exit look like for technology companies; topics that GNI will continue to explore through shared learning. To create space for those discussions, during this assessment cycle, GNI created two new working groups: one focused on sharing lessons and facilitating learning around human rights due diligence; and another focused on understanding responsible tech company conduct in situations of armed conflict.

THE FOLLOWING IS AN OVERVIEW OF THE TYPES OF DEMANDS THAT COMPANIES FACE

TYPE OF PRESSURE	DESCRIPTION	IMPACT ON FREEDOM OF EXPRESSION AND/OR PRIVACY
User or content-specific demands	The "original" form of demand, these focus on specific content or accounts.	When not properly issued, scoped, or applied, these can negatively impact FOE & privacy.
Network disruptions	Compelled complete or partial shutdowns of communications networks or the blocking of entire platforms or services.	In practice these blunt tactics are almost always unnecessary to achieve the stated government objective, & result in disproportionate impacts on freedom of expression & other rights.
Terms of service (ToS) requests	Requests by government authorities and/or government-directed actors to restrict content based on company ToS. This includes requests made by "**Internet Referral Units**" & through "trusted flagger" mechanisms.	When conducted in a coordinated and/or surreptitious manner, they can overwhelm response processes leading to FOE restrictions on targeted users.
Open-source surveillance	Efforts by governments to surveil expression in public or private digital spaces.	When conducted in a discriminatory manner or not accompanied by sufficient oversight, accountability, & transparency, can result in discrimination, privacy infringements, & chilling of association and expression.
Jawboning	Threats of legislation, prosecution, or other adverse actions against companies intended to compel compliance with government requests or demands.	When not sufficiently transparent or when explicitly tied to inappropriate government demands, can have negative FOE and privacy impacts. These impacts are especially likely where democratic oversight & accountability mechanisms are weak.
Data localization	Requiring that data be stored within a particular jurisdiction.	Often associated with an increased likelihood that the government will demand or otherwise seek access to stored data in ways that could infringe on privacy. Can also create chilling effects on expression.
Personnel localization (aka "hostage provisions")	Legal requirements that compel companies to hire or place personnel in a specific jurisdiction for the purposes of responding to government requests & demands.	Telecom & internet service providers have long had to contend with governments pressuring local employees to comply with demands, including inappropriate threats against their personal liberty & security. In recent years, these provisions have led to similar pressure against employees of internet platforms & services.

TYPE OF PRESSURE	DESCRIPTION	IMPACT ON FREEDOM OF EXPRESSION AND/OR PRIVACY
Direct access (see GNI definition and description **here**)	Legal & technical arrangements that allow government actors to access data streams directly, without having to request access from, or even notify, service providers that collect and/or transmit the data. Often carried out pursuant to secret/non-public laws, licenses, or orders.	When not subject to appropriate legal procedures, oversight, accountability, or transparency and/or carried out using non-standardized lawful interception solutions, they are likely to infringe on privacy.
Direct censorship	Legal & technical arrangements that allow government actors to filter, censor, or otherwise restrict content directly, without having to request action by, or even notify, the service providers that facilitate and/or transmit the content.	Although rare, technology offering this sort of control is increasingly available. Direct censorship by governments is very challenging to reconcile with legality, necessity & proportionality principles & therefore likely to violate freedom of expression.
SIM/device registration	Laws or regulations mandating that manufacturers, retailers, or service providers collect customer information so it can be provided to the government.	Often unnecessary to achieve the stated government objective & likely to lead to disproportionate infringement on privacy. Can also chill exercise of freedom of association & expression.
Compelled speech	Government demands that companies add or distribute specific content on or through their communications products or services. This includes content requirements intended to address "disinformation," as well as mass SMS requests.	When not sufficiently tailored, lacking appropriate legal authority, or not accompanied by sufficient accountability & transparency measures, compelled speech can violate freedom of expression.
Spyware & other forensic tech	Software & hardware that allow for access to and/or manipulates user devices or accounts.	Use of these powerful tools without sufficient and appropriate legal, oversight, transparency, and accountability frameworks leads to privacy infringement.
Data purchasing	Acquisition of data from third-party data brokers.	Where done without sufficient authorization, oversight & accountability safeguards, & transparency, these purchases & subsequent uses of purchased data can infringe on privacy.
Fake companies, apps, & accounts	Use of front companies, consumer- targeted apps, or fake accounts that are surreptitiously run or controlled by government actors.	Often used to acquire restricted technology, collect user data, and/or to promote government propaganda, in ways that would not otherwise be legal or consistent with international human rights principles.

OPPORTUNITIES

While underscoring the challenges that tech companies face in respecting freedom of expression and privacy, the assessments also point to a wide range of successful advances, innovative approaches, and strategic opportunities. At the most basic level, the assessments tell the story of how GNI member companies have prioritized human rights through explicit policy commitments, dedicated human rights functions and teams, senior-level engagement and oversight, expanded training, and more accessible grievance mechanisms. By integrating human rights awareness across relevant business units, products, services, and functions, these companies have positioned themselves to more effectively identify and mitigate human rights risks. Innovative uses of technical tools, expert advice, and third-party resources, have allowed companies to scale and focus their human rights due diligence efforts in ways that help them preempt, prioritize, and respond to relevant impacts, even as the "threat surface" of government restrictions expands.

Beyond these internal steps, the assessments also illustrate how successful risk assessment and mitigation depends on stakeholder engagement, cross-sectoral collaboration, and coordinated advocacy. GNI is already a central mechanism for such engagement, collaboration, and coordination, and is committed to doing more to enhance trust, facilitate shared learning, and expand policy advocacy in response to the external challenges identified above.

The assessments also help illustrate the wide range of products, services, and business models that GNI member companies are responsible for beyond traditional platform and telecom services. These include:

- App stores
- Business-to-business services
- Cloud services
- Consumer software
- Cybersecurity services
- Data storage products and services
- Drones
- Internet of Things infrastructure and services
- Location services
- Network equipment
- Managed services

One important lesson that GNI has taken away from this cycle is the need to better educate members and outside stakeholders, including governments, about the differences and relationships between these distinct businesses. One illustration of our expanded efforts along these lines is the "**Across the Stack Tool**" that GNI produced through its HRDD Working Group and in collaboration with Business for Social Responsibility. This tool, developed with support from the Dutch Foreign Ministry, is designed to help actors working across the technology ecosystem identify and address high level human rights issues and due diligence "questions." It builds off of discussions in the GNI assessment context and in the HRDD Working Group about how risks can be easier to identify and mitigate when actors share understandings about the interactions between different technology products and services, and their associated design and governance.

Another important lesson illustrated in these assessments is the centrality of meaningful stakeholder engagement to well functioning HRDD approaches. But as more companies seek to engage knowledgeable and credible stakeholders on a wider range of products and services, these laudable efforts are generating concerns about the lack of coordination among companies in their outreach, "engagement fatigue" on the part of some stakeholders, power imbalances, and the lack of meaningful follow-up. GNI is well positioned to help address these concerns and will continue to explore ways to improve individual and collective company engagement. One example of how GNI has leveraged its expertise, in order to inform and better position civil society for engagement with companies, is the **How to Guide on Engaging Tech Companies on Human Rights**. This tool, which GNI developed with Global Partners Digital with support from the U.S. State Department, identifies a series of best practices based on learnings from GNI assessments, as well as illustrative case studies drawn from the experiences of certain GNI civil society members.

This assessment cycle also helped underscore the important role that GNI companies are playing in not only developing cutting-edge technology, but also proactively seeking to identify and

address the risks they may present. GNI members have been at the forefront of fostering understanding around new technologies like 5G and AI, including through public explainers, dedicated HRIAs, and engagement in related standard setting processes. Going forward, GNI will continue to facilitate shared learning around new technologies, as well as more cross-stakeholder collaboration to center human rights in relevant multilateral and multistakeholder processes focused on these technologies.

This assessment cycle has also shown how well-functioning HRDD systems can identify and help mitigate a wide range of potentially negative impacts, even when they are designed to focus on a narrower set of human rights concerns. Examples include impacts identified and/or addressed in research and development and product development stages. HRDD risks can also help identify non-human rights risks related to suppliers and other third-parties, as well as unintended uses of relevant products. These observations underscore the importance of integrated, holistic HRDD and illustrate the limitations of approaches that attempt to distinguish rigidly between "upstream" and "downstream" risks.

Finally, the assessments revealed some unintended consequences of well-intentioned policies. This can be especially challenging in the context of company transparency efforts. While GNI members agree with the importance of transparency as a means for facilitating awareness and accountability, it is also the case that transparency can sometimes contribute indirectly to negative human rights outcomes. As a means to foster further discussion around these issues and enhance the role of global majority actors in critical transparency efforts, the GNI worked with a range of partners to develop and launch the **Action Coalition on Meaningful Transparency** (ACT). The ACT, which was launched as part of the Danish government's Tech for Democracy initiative and received support from the Omidyar Network, involves a wide range of GNI members and other civil society partners and is fostering critical research projects, as well as the development of a transparency portal.

> The digital regulatory landscape is constantly changing. And with the evolution of new government-led mandatory due diligence processes, we have to continuously evolve our internal assessment mechanisms to ensure our most salient human rights issues are identified and addressed. GNI's assessment process provides a safe, secure and collaborative space to tackle these difficult dilemmas on human rights in the digital age, and helps us, and all other participating companies, to constantly refine our processes. It is a testament to the power of collective effort in preserving users' rights.
>
> EMIL LINDBLAD KERNELL, Ericsson

7.

Looking Ahead

7. Looking Ahead

One important trend illustrated in this assessment cycle is the emergence of government mandates that require companies, including technology companies, to "know and show" how they respect human rights. Assessments of companies like Orange, which was subject to the groundbreaking French Duty of Vigilance law, and others who were preparing to comply with similar laws, illustrate the challenges and opportunities these laws present for GNI going forward.

On one hand, as illustrated in Orange's assessment, companies that are implementing the GNI Principles are well positioned to comply with mandatory HRDD laws. The substantive overlap between the core components of the GNI Principles, Implementation Guidelines, and the assessment framework – governance, due diligence and risk management, transparency and engagement – ensure that GNI companies are making necessary commitments and building robust internal systems, which can address a wide range of scenarios, including but not limited to government demands and restrictions. And GNI's focus on freedom of expression and privacy ensures that these companies are appropriately addressing two of the most salient areas of risk for technology companies.

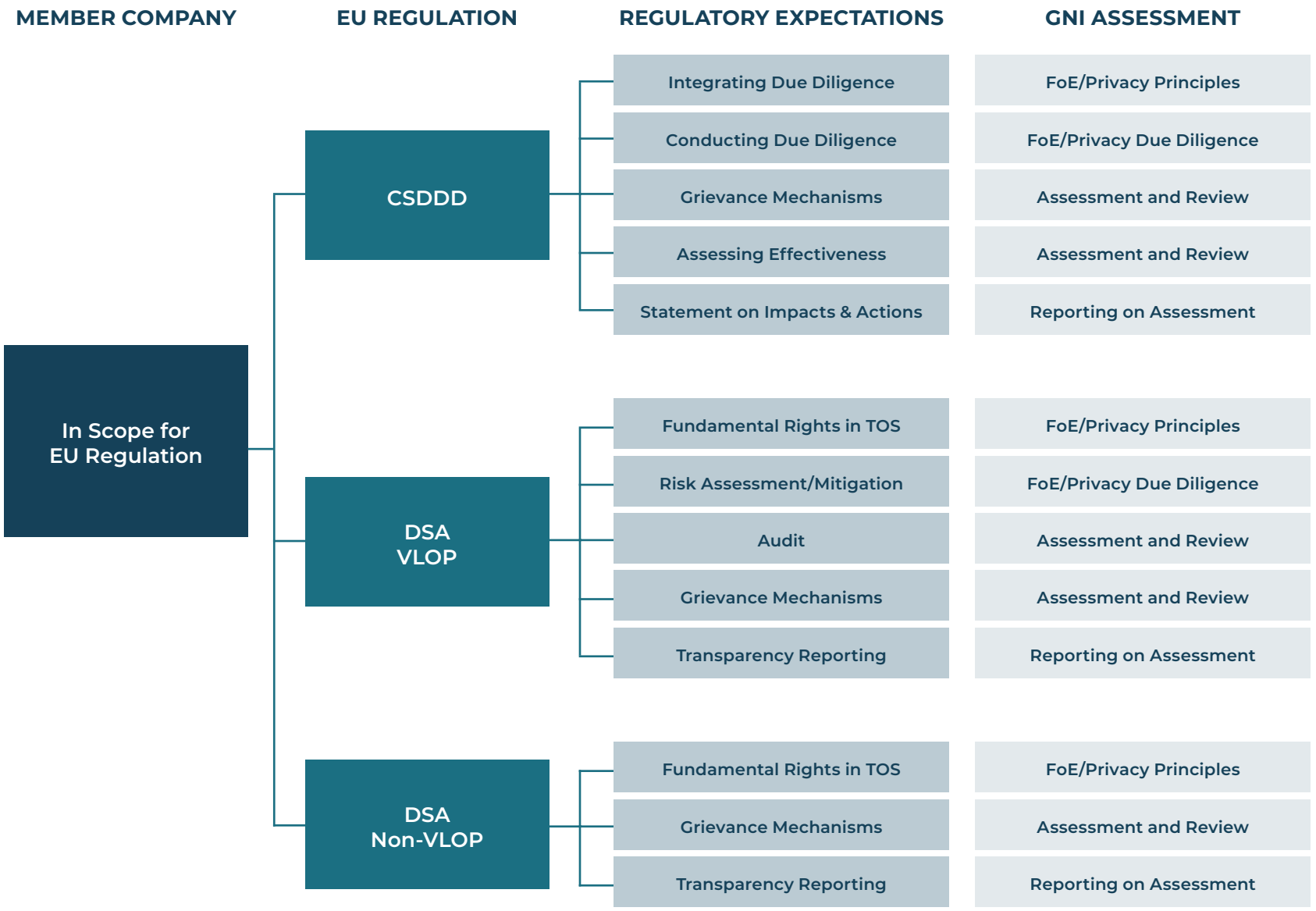
On the other hand, there is a risk that these new laws, if not sufficiently aligned with international human rights standards and widely-accepted good practice and guidance, could create confusion and uncertainty. In addition, if compliance is watered down or under enforced, there is a risk that it will create a low ceiling, rather than a high floor. As companies prioritize attention and resources on meeting mandatory targets, it is possible they will deprioritize multistakeholder initiatives and other collaborations that have meaningful positive impacts but don't translate as well into easy to quantify compliance metrics.

The overlap between these broad, sector-agnostic mandatory HRDD laws, and other digitally-focused laws like the EU Digital Services Act, which also create risk assessment and audit requirements, only underscores the importance of aligning around the international human rights framework and working collaboratively to understand and iron out inconsistency between the approaches of different jurisdictions. The tables on the next three pages - one from a report commissioned by GNI and the other from our friends at the Danish Institute for Human Rights - outline some of these laws.

GNI has advocated for and welcomed these regulations and is working hard to shape expectations around their implementation. And we will evolve our assessment process, as we have between every cycle, so that it continues to reflect and reinforce best practice in the technology sector, while seeking efficiencies and complementarity with emerging, rights-respecting regulatory requirements. We look forward to working with our members, assessors, and others to continue to evolve the GNI assessment framework and maximize our impact on privacy and freedom of expression.

HRDD/AUDIT REGULATION AND GNI ASSESSMENT

GNI has been exploring how assessment can be better adapted to emerging regulatory expectations and outputs. The chart below was developed by Article One consultants to show how different regulatory requirements intersect with the GNI Assessment.



SUMMARY OF EU MEASURES RELATED TO BUSINESS AND HUMAN RIGHTS, PUBLISHED BY THE DANISH INSTITUTE FOR HUMAN RIGHTS ON 30 AUGUST 2023

MEASURE	NATURE	STAGE	REFERENCE TO BHR FRAMEWORKS	DUE DILIGENCE	REGULATORY ALIGNMENT
Proposed Corporate Sustainability Due Diligence Directive (CSDD Directive)	Due diligence obligation and corporate governance reform	Proposal launched February 2022. The Council adopted its negotiating position (general approach) in November 2022, which departs from the Commission's proposal in a few key respects. Trilogue negotiations between the European Parliament, the European Council, and the European Commission could begin as early as May 2023.	Multiple references and overall ambition to align with key International frameworks, including the UNGPS and OECD Guidelines.	Contains due diligence requirements that broadly align with due diligence steps from UNGPS and OECD Guidelines but depart from these frameworks on several accounts.	Broad due diligence requirements will need to be considered alongside other sectoral due diligence initiatives such as the Conflict Minerals, Timber, Batteries, Forced Labour, and Deforestation import controls. CSDD Directive relies on CSRD for associated disclosures. Unclear how it relates to SFDR, including if and when covering financial sector companies. Unclear how it will interact with taxonomy regulation Article 18.
Corporate Sustainability Reporting Directive (CSRD)	Reporting requirement	CSRD proposal was published in April 2021 and entered into force on 5 January 2023. Member States are expected to transpose the Directive into national law 18 months after it enters into force	The CSRD aims for consistency with international instruments such as the UNGPS, the OECD Due Diligence Guidance for Responsible Business Conduct and related sectoral guidelines, the UN Global Compact, the ILO Tripartite Declaration, ISO 26000, and the UN Principles for Responsible Investment	Requires disclosure of the due diligence process implemented, but does not itself require the exercise of due diligence or alignment with RBC standards	CSRD to serve as the reporting obligation associated with CSDD Directive. CSRD is also key to taxonomy, alignment reporting. including on article 18. Unclear how the disclosure requirements will align with the SFRD disclosure obligations on financial market participants.

MEASURE	NATURE	STAGE	REFERENCE TO BHR FRAMEWORKS	DUE DILIGENCE	REGULATORY ALIGNMENT
Digital Services Act (DSA)	Rules on digital services	The proposal was published on 15 December 2020. The EU Parliament adopted amendments to the proposal on 20 January 2022. It was published in the Official Journal of the European Union on 27 October 2022, entered into force on 16 November 2022 and will start to apply from 17 February 2024 for all regulated entities.	The recital of the DSA states that all providers of intermediary services should pay due regard to relevant international standards for the protection of human rights, such as the UNCPS.	It is not framed as a human rights due diligence framework, but it emphasises the need for intermediary services providers to ensure their activities protect human rights online, including the right to privacy, freedom of expression and information, prohibition of discrimination, and vulnerable users. It also requires more due diligence obligations to manage systemic risks for very large online platforms and very large online search engines.	The due diligence obligations in the DSA are both sector-focused and narrower in scope than the UNGPS and the broader due diligence obligations in the CSDD Directive. The reporting requirement under the DSA, which includes information on human rights-related risk assessment and mitigation measures, will also need to be considered alongside the disclosure requirements in the CSRD.
Proposed EU Artificial Intelligence Act (AI Act)	Law on Artificial Intelligence	The Commission published a proposal to regulate artificial intelligence in the European Union in April 2021. The Council adopted its general approach in December 2022. The proposal will follow a full legislative process at the EU Parliament and Council of the EU before being formally adopted.	While there are no explicit references to the UNCPS in the AI Act, several of the UNGPs' due diligence requirements are partly addressed by the proposals text. Also, the adverse impacts that AI caused on fundamental rights, including the right to privacy, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non- discrimination, consumer protection, workers' rights, rights of persons with disabilities, rights of children, are acknowledged in the proposal.	While it is not framed as human rights due diligence framework. the proposed AI Act aligns with the UNGPS approach to due diligence in identifying, preventing. and mitigating potential or actual adverse impacts connected to an activity. It requires adopting a risk management system in relation to high-risk AI systems.	The alignment of the AI act with the due diligence obligations within the proposed CSDD Directive should be ensured. The disclosure requirements in the AI Act will also need to be considered alongside the disclosure requirements in the CSRD. The AI Act does not affect the application of the provisions of DSA and GDPR.

Annexes

Annex 1: Acronyms and Abbreviations

AI	artificial intelligence
ACT	Action Coalition on Meaningful Transparency
AOL	America Online, Inc.
ARM	Assessment Review Meeting
AR	Manual Authority Request Manual
AROC	Audit and Risk Oversight Committee
BHRP	Business and Human Rights Program
CELA	Corporate and Legal Affairs
CEO	chief executive officer
CCO	Chief Compliance Officer
CSR	Corporate Social Responsibility
CSWG	Case Selection Working Group
DPIA	Data Protection Impact Assessment
DSA	European Union's Digital Services Act
ESG	environmental, social, and governance
ETNO	European Telecommunications Network Operators
ETSI	European Telecommunications Standards Institute
EU	European Union
FAQ	frequently asked questions
5G	fifth generation of cellular communications
FISA	Foreign Intelligence Surveillance Act
FOE	Policy Microsoft's internal Freedom of Expression Policy
GEM	General Executive Management
GREC	Governance Risks Ethics and Compliance forum
GDPR	European General Data Protection Regulation
GNI	Global Network Initiative
GREC	Governance, Risk, Ethics, and Compliance
HRDD	Human Rights Due Diligence
HREC	Human Rights Executive Council
HRIA	Human Rights Impact Assessment
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IoT	Internet of things
ITU	International Telecommunication Union
LEA	Law Enforcement Agency
LENS	Law Enforcement & National Security
LERA	Law Enforcement Response Analyst
LLP	Limited Liability Partnership
MANA	Market Area North America
MELA	Market Area Europe and Latin America
MMEA	Market Area Middle East and Africa
MNEA	Market Area North East Asia
MOAI	Market Area South East Asia, Oceania and India
M&A	Merger and Acquisition
NATO	North Atlantic Treaty Organization,
NGO	non-governmental organization
NSIPGC	National Security and Investigatory Powers Governance Committee
OECD	Organization for Economic Co-operation and Development
SCC	Sustainability and Compliance Committee
SCP	Supplier Conduct Principles
SPOC	single point of contact
3GPP	3rd Generation Partnership Project
UN	United Nations
UNGPs	United Nations Guiding Principles on Business and Human Rights
U.S.	United States
VOIP	voice over Internet protocol

Annex 2: Case Studies

Each GNI company typically includes at least eight case studies as part of their assessment report. These cases help GNI assesses whether and how the company's systems, policies, and procedures were implemented in practice, particularly when responding to government requests and demands. Case studies also help the GNI Board track progress and monitor whether a company is making good-faith efforts to implement the GNI Principles with improvement over time.

In total, this assessment cycle included the examination of 88 cases in a variety of operating environments, including specific responses to government demands, as well as cases regarding the broader context of company operations. This supplement to the broader **Public Assessment Report for the 2021-2022 GNI assessment cycle** provides a summary of 26 selected, anonymized and non-anonymized cases from the company assessment reports produced as part of that cycle.

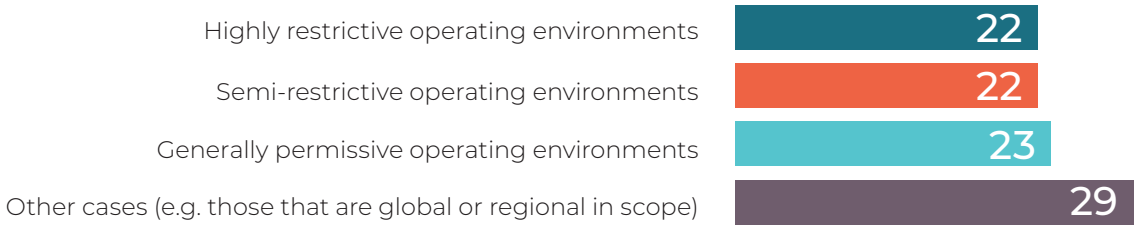
Just as the cases selected for inclusion in each assessment report are not a statistical sample of the thousands of government demands that GNI member companies receive, the cases in this supplement are not necessarily representative of the cases included in this cycle overall, since many of the most sensitive cases are not included. In addition, each of the cases included here have been abridged and edited to omit particularly sensitive details, both regarding the underlying cases and the discussions that they may have helped to spark. These cases nevertheless cover a range of topics and regions and demonstrate the different types of government requests that companies must navigate in a variety of circumstances and contexts.

KEY THEMES, OBSERVATIONS, AND LEARNINGS INCLUDE:

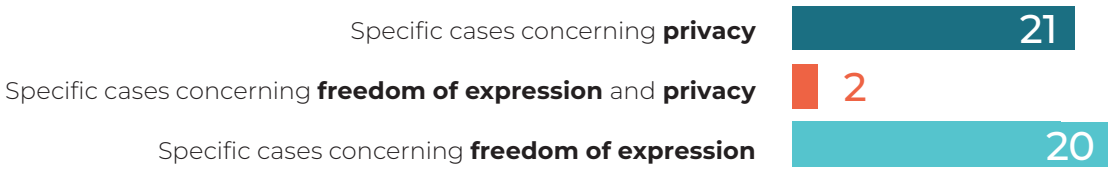
- **Covid-19:** The types of government requests companies faced during the Covid-19 pandemic and how they responded through policy and process.
- **Regulatory pressure:** Increasing regulatory pressures on companies through a range of instruments including licensing regimes, intermediary liability rules, and restrictions on foreign direct investment.
- **Government requests:** The different avenues and techniques companies used to respond to and mitigate the impacts of government requests that could have negative impacts on the right to privacy and freedom of expression. Companies faced a range of requests including access to data, removal of content, correction of content, requirements to implement technical capabilities, and requests to update technical system components. Company responses highlighted the integral role the relevant internal policies, processes, and teams play in assessing and responding to such requests.
- **Identifying and addressing misuse of products:** Using Human Rights Due Diligence (HRDD) policies and processes to identify and address potential vulnerabilities in their products and the misuse of the same.
- **Importance of external resources:** Reaffirming the importance of the research and work developed by external actors including CSOs and academics, companies used external resources to better understand contextual situations and inform policy development and HRDD-related decisions.

OVERVIEW OF CASES

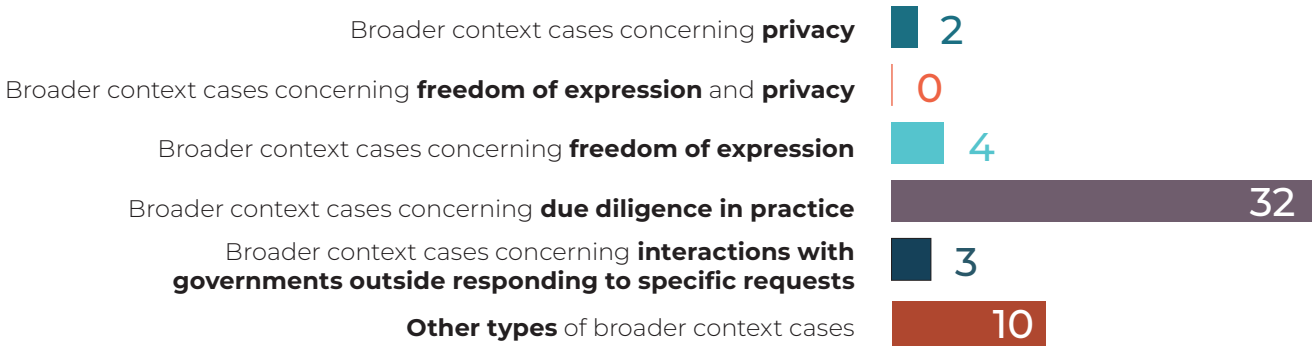
CASES BY OPERATING ENVIRONMENT



CASES INVOLVING A SPECIFIC GOVERNMENT REQUEST: 39



CASES RELATED TO THE BROADER CONTEXT OF COMPANY OPERATIONS: 44



This graphic was developed from and represents the 88 case studies that were reviewed during the fourth GNI assessment cycle.

Case Examples

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

Request to enable an in-country server for authorities in a country in Eurasia to collect location data in emergency situations

This case examined the use of Nokia's solution in a government-hosted, multi-operator environment whereby an in-country server would enable the operator to collect precise location data, send it to a control point in the operator network, and then forward it to government authorities in the event of an emergency call initiated by a subscriber.

According to its **Human Rights Policy**, "Nokia will provide communications systems, drones, video transmission, and other networking capabilities to governmental and enterprise customers for purposes such as public safety, transport, energy and smart city enablement. Nokia will not pursue business with intelligence agencies or entities that work on active surveillance or the interception of communications."

Based on these conditions, Nokia's human rights due diligence (HRDD) panel investigated the technical set-up, including the government authority's access to specific data. The HRDD panel determined that the government authority would only receive the location of the emergency caller after the call had been initiated, with no other information being sent. The government authority would not be able to monitor anything other than the location of the emergency call. Based on its review, the HRDD panel determined that this transaction was a "Go With Conditions."

This case study provides a useful illustration of Nokia's investigative process, specifically how this process requires a precise understanding of the technology at issue and its potential use. It also provides a helpful example of a decision to proceed with a transaction only after certain conditions are met, illustrating that the HRDD panel's decisions are not always, and need not be, binary.

Government requests for assistance during the Covid-19 pandemic

This case examined a number of different, unconventional requests from governments to Telia Company for assistance related to the Covid-19 pandemic.

The company's 2020 sustainability report outlines its commitment to transparency during the COVID-19 pandemic, detailing government requests and responses. Telia assisted various countries in COVID-19 initiatives, including blocking fraudulent sites, sending mass SMS, and supporting apps. The report covers actions taken in Denmark, Estonia, European Commission collaboration, Finland, Latvia, Lithuania, Norway, and Sweden. The report demonstrates that Telia emphasized adherence to GDPR and privacy laws, while working with authorities to fight the pandemic. In September 2021, local companies confirmed that no further of such requests had been noted.

This case combines several unconventional requests related to restricting and blocking access to Covid-19 related information, for which Telia had clear procedures.

Singapore POFMA Order

On 22 January 2020, Yahoo received a request from the Singapore government to issue a correction notice under the Protection from Online Falsehoods and Manipulations Act (POFMA). The request identified an article published by one of Yahoo News Malaysia's partners, and highlighted five of the article's statements that the government was contesting. The notice also included the prescribed text for a correction notice.

Once the local legal team received the request it was escalated to the regional counsel. This regional counsel then escalated the case to Yahoo's General Counsel, VP for Global Public Policy, APAC Policy Lead, and BHRP, including her recommendations on how to proceed. The policy team and BHRP then discussed the human rights impacts of the request. It was agreed that Yahoo would need to comply with the law but that there was some leeway available in how it did so.

To better understand the situation, Yahoo engaged outside resources to analyze previous uses of the POFMA correction notice. The policy and BHRP teams then put forward additional wording to add to the correction notice which would clarify that Yahoo was acting under legal obligation and did not dispute the underlying reporting. After internal meetings were held and all approvals were received, Yahoo listed the required correction with an additional explanation of why the company was issuing the correction.

This case study illustrates the challenges that organizations like Yahoo have in upholding their human rights commitments while complying with lawful processes that might be incompatible with, or even hostile to rights of privacy and free expression. It also demonstrates the ways in which companies can attempt to mitigate the impacts of compliance when necessary.

Development of COVID-19 contact tracing application

As France entered its first Covid-19 lockdown, Orange collaborated in the development of an application that would trace – and not track – contacts between people in order to identify potential Covid-19 exposures. The product development followed Orange's own processes relating to privacy by design and benefited from the oversight of a cross-organizational working group and French authorities.

In March 2020, Orange identified Bluetooth Low Energy (BLE) as the most suitable connectivity solution for assessing the proximity of individuals. Collaborating with industry partners, it contributed to the "Stop Covid" project initiated by the French government in April 2020, aiming to develop a secure, privacy-respecting, mobile-based solution for contact tracing using BLE. The project adhered to French laws and European regulations. The developed app prioritized data protection and privacy. The company created a Captcha module that does not collect personal data, which is used by various of Orange's clients.

This case demonstrated how having appropriate due diligence procedures in place can allow a company to respond to unforeseen emergencies in an innovative and rights-respecting manner. It also illustrated the importance of data protection legislation on the robustness of privacy due diligence in product development.

ERICSSON

Solution request of a local operator in South Asia

This case involved Ericsson receiving a solution request from a local operator in South Asia in relation to a core network opportunity. As part of the overall request, the local operator requested a solution that records subscribers' activities on the network, which includes their website history, as required under the country's telecommunications licenses. The solution and data collected would be used by the local operator for, among other things, data sharing with local authorities. Completing this request would require Ericsson to complement its core network proposal with a third-party product. Ericsson used the Ericsson Code of Business Ethics, the Ericsson Business and Human Rights statement, and the Ericsson Sensitive Business Group Policy and Sensitive Business Group Directive to analyze how to proceed.

Ericsson responded to this solution request by following its standard Sensitive Business process, identifying elevated risks related to the right to privacy. Further, after conducting a thorough technical evaluation of the third-party equipment and analysis of the local legal framework, Ericsson determined that adhering to the request would come with a high risk of negative impacts on the right to privacy in the country. Ericsson decided not to integrate the third-party component in order to avoid unrestricted data sharing with authorities. The remaining part of the core network request was conditionally approved with contractual mitigations.

The assessor for this case study determined that Ericsson respected the GNI principles related to privacy rights and properly followed the Sensitive Business Policy processes. This case exemplifies the importance of the relevant internal policies and processes for identifying human rights risks, and then enabling decisions that can mitigate those risks.

Due Diligence during the sale of Telenor Myanmar

This case focused on Telenor's due diligence and decision-making process during the sale of Telenor Myanmar following the February 2021 military coup.

Immediately after the February 2021 military coup, Telenor established a Crisis Management Team, with a Steering Committee representing management from key areas of the company. This group and the Board met regularly to receive information and consider options. Over the course of the next several month, Telenor took multiple public steps in response to the evolving situation on the ground in Myanmar, including: setting up a tracker on its website indicating the status of the network; condemning violence against the people of Myanmar; protesting the draft Cybersecurity Law that was put forward soon after the coup; signing statements, including GNI's statements; engaging with stakeholders, including through a session organized by GNI and the Myanmar Centre for Responsible Business; providing transparency to users including via local website, social media, and SMS channels; and creating a dedicated website providing updates on the situation in Myanmar. It also took steps internally, including: holding regular meetings with local staff; communication with staff through various internal channels; and providing legal and other support to employees.

Telenor also undertook human rights due diligence (HRDD) and impact assessments to examine its options, including remaining in Myanmar and selling. This HRDD took into account the potential impacts on a range of rights-holders, including employees, customers, distributors, vendors and partners in Myanmar. A range of risks were identified, including related to: the safety and security of Telenor Myanmar personnel; customer privacy, security, and safety; domestic and international legal compliance; and forced activation of lawful intercept (LI) systems.

After conducting this research, Telenor decided that continuing operations in Myanmar under Telenor control would not be possible for various reasons, including the military regime's insistence that LI equipment be activated, which Telenor determined would violate its policies and legal obligations. Once Telenor determined that remaining in Myanmar was not viable, it explored different options for effectuating its exit. Of these, sale was determined to be the most feasible and least detrimental option, as it would maintain connectivity for customers and protect local jobs and livelihoods. Five months after the military coup by selling Telenor Myanmar to M1 Group.

This case study provided a useful window into the types of decisions and dilemmas that companies face in the wake of a sudden regime change and in a conflict environment. Telenor had engaged with GNI and its members throughout the process, and the case provided a great understanding of ways in which GNI can support members in these types of situations.

NOKIA

Interface changes related to lawful interception in a Latin American country

This case looked at how Nokia handled a situation in which a government authority requested operators to make minor interface changes related to lawful interception due to an outdated setup.

According to Nokia's policies, the company will provide passive lawful interception capabilities to customers who have a legal obligation to provide such capabilities. This means that Nokia will provide products that meet lawful intercept capability standards. Nokia will not engage in any activity relating to active lawful interception technologies, like storing, post-processing or analyzing intercepted data gathered by the network operator.

For Nokia, this request was addressed via a standard human rights due diligence (HRDD) investigation. This investigation focused on whether there would be any changes to the capacity requirements of the equipment. The HRDD process concluded that the project was a "Go" after determining an upgrade was required for the next version of the previously supplied equipment.

According to Nokia, this was a typical request relating to the implementation of the company's Human Rights Policy, because this technology would not alter Nokia's involvement with the Lawful Interception system. The system would remain passive and Nokia would not be instructed to take any actions by a governmental authority. There would also be no storage or post-processing activities.

While this case does not present a novel question, the assessor noted that it illustrates how robust Nokia's HRDD process is for even ordinary equipment upgrades where no changes to standard Lawful Interception technology are contemplated. Nokia still runs the upgrade through the diligence process to ensure that it understands what the technology it is providing can do and to be certain that it is acting consistently with its Human Rights Policy.

ANONYMIZED

Emergency request for user data from a European government

In March 2021, a GNI company received an emergency request from the police in a Western European country in connection with a dangerous sex offender who had escaped from prison. In response to the request, the company provided registration information.

According to the company's relevant policies, the company does not provide governments with customer data until a relevant legal demand mandates it. Such requests are first reviewed to ensure their validity and to evaluate that disclosure is necessary to address an emergency that involves the danger of death or serious physical injury to a person.

The company's policy notes conditions that must be met for law enforcement requests to be considered, including that it must be in writing and signed by an authorized official, and that it must outline the nature of the emergency and how the information sought will assist the law enforcement agency in question in addressing the emergency. The company discloses the least amount of data it believes will help the law enforcement agency in addressing the emergency. In this case, after reviewing the request, the company provided a limited amount of user information (basic registration data) only after verifying the legitimacy of the emergency request.

This case illustrates how the company processes emergency requests from law enforcement and helps demonstrate how compliance with such requests can be both timely and considered.

Data Sharing request during COVID-19

This case examined how British Telecommunications responded to a request from the UK Government asking BT to provide the UK with aggregated and anonymized mobile data, in order to help them determine and implement a COVID-19 strategy. Specifically, the UK Government requested data that covered the movements of the population at large so that the Government could generalize movement patterns and plan a public response to COVID-19.

In response, BT undertook a review by several internal stakeholders, including representatives from the Data Solutions, Public Policy, Technology, Human Rights, Legal, Security and Data Protection teams. BT participated in various industry groups, including Global Network Initiative, Mobile UK and GSMA. In addition, it reviewed the guidance from the ICO and the EDPB. BT also assessed the various COVID-19 approaches taken by mobile operators in other countries. The company undertook a full data protection impact assessment, implemented multiple measures to protect data and ensure that data being provided could not be reverse-engineered, and then responded by providing the Government with a limited amount of aggregated and anonymized data. BT also took a number of steps to be transparent with its users about the data sharing.

This case demonstrates how relevant processes and teams can work together to be responsive to a legitimate government demand in a time-sensitive manner, while fully considering and working to mitigate potential human rights risks.

Navigating government restrictions on freedom of expression

The case refers to two service restriction/shutdown demands that took place in the same country and the company's response to the same. The first restriction took place during a referendum, while the second took place after an election.

In the first instance, the Orange local CEO received a call from the government's Telecom Regulator demanding an immediate slowdown of traffic on Facebook and Twitter. The Regulator also demanded the filtering of Facebook and Twitter traffic. The CEO requested a written order and did not comply until receiving one via SMS. A legal review of the request was carried out and Orange corresponded with NGOs about the incident. Orange did not proactively communicate to customers during the restrictions.

Not long after, Orange faced another government demand to throttle Facebook at 90% capacity. The demand also sought to throttle the entire internet on the night when the election results would be announced. After Orange did not comply with the order, the company's IP access to the submarine cable was disconnected, affecting mobile internet and international calls. Orange informed its minority shareholders, the French government, and GNI of the situation. It also wrote to government officials requesting information as to why its access to the submarine cable had been disrupted. Confirmation of government involvement came two days later via a public communication, prompting the company to release a press statement attributing the shutdown to an international access point issue. The disruption persisted for six days.

This case illustrated the company's application of the GNI Principles to navigate government restrictions on freedom of expression, and the difficult decisions that companies face in unstable political environments. In this case, the company's unwillingness to throttle service in line with the demand likely led to targeted disconnection, limiting its options to mitigate the impact of the restriction.

Google

Responding to administrative subpoenas

From January 2020 through June 2020, Google received nearly 40,000 requests for user information from law enforcement agencies in the United States — more than 15,500 were subpoenas, according to an annual transparency report. Google provided some data in 83% of cases arising out of these subpoenas. Several civil rights and legal groups worried that federal agencies could use legal processes such as administrative subpoenas to gain access to user information to expand surveillance of U.S. residents. Google has a policy of notifying users of government requests, including those from the US Department of Homeland Security's Immigration and Customs Enforcement agency (DHS/ICS), seeking information related to their Google account, unless prohibited by law.

Requests from DHS/ICE have sought sensitive personal information such as: names, email addresses, phone numbers, Internet Protocol addresses, street addresses, length of service such as start date, and means or sources of payment linked in any way to the Google account. Per Google's policy, this information is produced to DHS/ICE within 7 days unless Google receives a copy of a court-stamped motion to quash the request after a user's successful appeal to the relevant court.

Consistent with Google's policies, Google will typically notify a user whose data is being requested and give them an opportunity to object to the request in the appropriate court unless there is a legal prohibition (such as non-disclosure order) restricting Google from doing so. Google will also make an effort to narrow requests for user data to limit or reduce the scope of what is being sought, if possible.

This case illustrates how Google seeks to provide notice to users whose information is being requested by a government agency, so that they may challenge those requests if they choose to. It illustrates the challenges that governments can impose on providing notice and the reasons why adherence to company policies consistent with the GNI framework, including transparency reporting, are important to users' rights.

ERICSSON

The role external reporting can play in corporate due diligence

Ericsson's Sensitive Business Core Team meetings include a section for any other business to allow meeting stakeholders to raise relevant topics not related to specific business opportunities. During this section of such a meeting, an NGO report about alleged surveillance in a Sub-Saharan African country was raised. The report alleged that telecom operators, which Ericsson had previously partnered with, were involved in facilitating government surveillance. The report also detailed the lack of appropriate safeguards in the country's laws.

On the basis of this discussion, a decision was taken to investigate if Ericsson's activity or equipment was in any way related to the alleged surveillance, and if so, whether the company's contractual mitigations had been followed. Local teams were engaged and multiple meetings were held. The analysis included a review of Ericsson's active customers in the country, the type of equipment installed, the purpose of the engagements, and the type of services provided. It was determined that Ericsson had provided standard telecommunication equipment not related to the equipment mentioned in the report.

This case highlighted the important role that external reporting can play in corporate due diligence and how changing circumstances over time can warrant a re-examination of the sensitivity of previous relationships and activities. It also exemplified how Ericsson's Sensitive Business process can help identify and respond to such situations, highlighting the importance of allowing for open discussion and consideration of situations that go beyond the examination of new business opportunities.

Responding to a request for collaboration on anonymous bomb threat

In February 2019, national authorities proposed a voluntary agreement with 3-5 operators, including Telia, for network shutdowns during emergencies like bomb threats. The company's policy emphasizes that it is necessary for governments to adhere to established domestic legal processes when seeking to restrict freedom of expression or access to personal information.

The company's local branch rejected the proposal, citing concerns about the rule of law, foreseeability, and transparency. They advocated for legislative initiatives and for public transparency for such measures. In November 2019, the company presented at a legal workshop emphasizing human rights, rule of law, and the necessity for legislation. As of Fall 2020, no further contacts were received, but the company assessed that the issue might reappear as draft legislation.

This case demonstrates how principled action by a company can cause governments to reconsider their own human rights obligations and help protect users rights.

Continuing Yahoo's business and human rights program

In May 2021, it was announced that Verizon was planning to sell the assets of the Yahoo and AOL brands to the private equity group Apollo Global Management. With this change, Verizon chose to retain the existing Business and Human Rights Program (BHRP) team, which had migrated to Verizon and become a centralized function within the company after Verizon's acquisition of Yahoo in 2017.

Yahoo's commitment to implement the GNI principles on Freedom of Expression and Privacy has been long overseen by the internal BHRP. The BHRP has set up a cross-functional team to conduct human rights due diligence, provide insights to business leaders and work with external stakeholders.

To prevent any gaps in Yahoo's continuation and commitment to human rights, its VP of Global Public Policy proposed to move the team into the Global Public Policy function under her oversight. The proposal was approved prior to the close of the sale.

To ensure a smooth transition, the incoming BHRP team met with the Verizon team on a weekly basis to transfer necessary knowledge. Concurrently, the new Yahoo BHRP team drafted language for a new BHRP page with a direct link on the Yahoo Corporate Homepage. The team also reviewed necessary policies to ensure that processes related to Yahoo's impact on Privacy and Freedom of Expression would continue without interruption.

After the close of the sale, the new Yahoo BHRP team was officially created. Since then, the team has been conducting internal audits, reintroducing themselves to various groups within Yahoo and presenting their work (including on the GNI Principles). The BHRP team also launched an internal website with updates on their work, contact information, and information regarding Yahoo's human rights commitments.

This case shows how Yahoo managed to support uninterrupted adherence to its human rights commitments in the face of significant, company-altering changes and could be a reference point for other companies going through similar transitions (acquisition, sale, devolution, etc.).

ANONYMIZED

Request for user data from a European government

In March 2020, a GNI company received a request from the regional police unit in a Western European country for the registration information of a user. The company did not provide any data in response to the request.

According to the company's policies, it does not provide governments access to customer data until a relevant law enforcement authority has issued a legal demand.

After receiving the request, the company's team reviewed it and found that while the request referred to suspicion of the person being guilty of one or more offenses, it did not state what the offense was. The company decided not to provide any information because of the vagueness of the grounds on which the data was being requested.

This case illuminates how the company's tiered approach can a) help filter out inadequate or non-specific requests and b) ensure a proper balance between protecting user privacy and supporting legal, necessary, and proportionate law enforcement activities. It shows that while the company takes legitimate criminal law enforcement needs seriously, it requires enough specificity to evaluate the validity of the requests and to respond in a way that is tailored and proportionate to the specified need.

orange™

Applying due diligence procedures to better understand contexts

Since 2012, Orange has worked with a third party to conduct human rights risk assessments for the countries where it operates. During this assessment period, Orange worked with the third party to strengthen the analysis in these assessments by providing additional consideration on government stability and civil unrest risk. In addition, the company began to juxtapose an election calendar against the results of the risk assessment.

Since 2012, twelve dimensions of human rights risk have been evaluated for each country and, then, an aggregate country rating is calculated. In 2020, Orange requested government stability and civil unrest as additional indices.

Orange also introduced a new step in its due diligence in order to juxtapose the country's risk analysis against the electoral calendar and identify where those events may lead to greater risk. As part of Orange's due diligence process, prior to election periods, special efforts are made by Orange to reduce and prevent risks to people and to Orange's business as a critical infrastructure operator.

This case is an example of how a company is applying due diligence procedures in evolving ways to better identify and understand contexts and events that may lead to heightened risk.

Pushing back on an overly broad removal request from the Ugandan Communications Commission

In Fall of 2020, the Ugandan Communications Commission ("UCC") engaged in a number of communications with Facebook, Inc. (now Meta Platforms Inc. - hereafter referred to as "Meta"), demanding the removal of certain content on Facebook. UCC also issued a directive to Meta to block access to Facebook Live in Uganda, alleging that the reported content and live videos were linked to domestic unrest and violence. After Meta's Content Legal Team assessed the situation, it was determined that the directive was made outside the scope of the UCC's power. Therefore, the company decided to not comply.

Meta follows a four-step process ("Company Process") in responding to formal government requests to remove/restrict content. In this case, the Content Policy team first reviewed the content identified in UCC's communications. While some content violated Facebook's Community Standards (and was removed globally), other pieces that did not were passed to Meta's Content Legal team for review. The Content Legal team, alongside outside counsel, was not able to determine that the reported content violated Ugandan laws on incitement to violence. Meta's Content Legal team ultimately found that the issuance of the directive was unlawful under Ugandan law, while the company's Public Policy team, in collaboration with its network of NGO partners in Uganda, discovered that the push for content restriction was politically motivated. Meta's cross-functional teams reviewed the directive from their GNI commitments perspective and in conjunction with the company's Community Standards and Human Rights Policy.

As a result of the assessment, Meta sent a letter to UCC confirming that it would not comply with the directive to block Facebook Live, as such a decision would result in disproportionate restrictions of lawful speech. After Meta's refusal, the Ugandan government ultimately ordered the blocking of the entire Facebook service in the country.

This case study points to how Meta's internal process led it to identify legal infirmities with and ultimately push back on law enforcement requests that were likely to infringe freedom of expression. This case also illuminates how engagement with locally-based NGOs helped Meta evaluate the political nature of the directive, and illustrates the significant consequences that can follow from a company's refusal to comply with government demands.

Request for information relating to a mission-critical 5G network

This case focused on a request for information for a mission-critical 5G network received from a national police force. This network would be used for police communication, camera surveillance, and national security operations. The network would be used to connect to surveillance cameras installed in public areas, which would send video signals back to a monitoring center. In the process of examining this request effectively, Ericsson referred to its Code of Business Ethics, Business and Human Rights statement, and the Sensitive Business Group Policy and Sensitive Business Group Directive. After reviewing this case within the Sensitive Business process, considering the customer and the situation and legal framework in the country, the request was denied.

This case highlighted the importance of conducting due diligence and illustrated the importance of working methods that foster communication between local or regional market teams and Sensitive Business process stakeholders.

Dissemination of information on Svalbard

The governor of Svalbard, a Norwegian archipelago and one of the northernmost inhabited locations in the world, requested the phone numbers of all inbound roamers in Telenor Norway's network in order to send them critical information on flights in the beginning of the COVID-19 pandemic. Because Telenor Norway considered this to be a request to access customer data, it referred to the Group Authority Request Manual to decide how to proceed.

The Manual was used as guidance and the request was escalated to Group Legal and the Telenor Norway Data Protection Officer, who determined that Telenor Norway had a legal obligation to complete the request and sent the list of phone numbers to the Governor of Svalbard. The Governor immediately sent SMS to all mobile numbers active on Svalbard with critical flight info (last flight leaving). Due to the time constraints Telenor was not able to send notice in advance to the customer that their numbers had been shared with the Governor.

This case demonstrated how new policies and procedures can be used even before they are fully implemented and illustrated the role of clear internal lines of communication, especially in the context of emergency requests and unforeseen circumstances.

Strengthening company whistleblowing processes

In June 2021, Orange launched a new outsourced, web-based whistleblowing platform "Hello Ethics," accessible to employees and external stakeholders. In the platform's first six months, one report was submitted that related to GNI issues.

'Hello Ethics" is an international, centralized service, open 7 days a week, 24 hours a day. The service provides the user with a clear view of their report's status; ensures that information remains confidential; and protects the whistleblower. After 6 months of activity of the system, it was found that there was: a very sharp increase in the number of messages received; filtering of out-of-scope messages; and a number of inaccurate assignment of submissions by whistleblowers. There was one report relating to GNI topics. In that report, the whistleblower claimed that Orange was allowing the secret service of the European country they were living in to tap their mobile phone line. Orange replied to the whistleblower that the case had been investigated and explained that it would only allow interception if demanded by competent authorities following due process.

The 'Hello Ethics' platform is an innovative approach that strengthens Orange's whistleblowing processes, including by allowing the company to identify trends over time.

Yahoo's Updated Community Guidelines

On 8 February, 2021, Verizon Media updated its Community Guidelines to provide greater transparency on how Yahoo (then Verizon Media) moderated content and clarity on what was and was not allowed on the platform.

Similar to the review process for product launch and end-of-life, new policies are also subject to an internal review process, which includes participation from the Yahoo Business & Human Rights Program (BHRP). In these reviews, BHRP is responsible for providing an assessment of potential human rights impacts and advising on potential mitigation strategies.

In this case, the BRHP team provided comments on the proposed new language and sought input from outside counsel on how to define certain terms like "terrorism." The team also organized an external consultation with the Center for Democracy and Technology (CDT) to review the proposed changes and solicit feedback. Once the updated guidelines were released, an internal blog was shared on The Street (the company's internal information website) to help employees better understand the policy and reasoning behind it.

This case study demonstrates how Yahoo works to maintain adherence to its human rights commitments and GNI principles even in the face of changes.

Group handing over to the new owner of Telia Carrier

In October 2020, Telia Company announced the divestment of Telia Carrier (now Aurelion) to Polhem Infra. In November 2020, the company presented to the new owner the range of ongoing human rights work in relation to Telia Carrier, which was to be carried on within Telia Company up until the divestment. In May 2021, the remaining open Telia Carrier issues in relation to freedom of expression and privacy were handed over to Telia Carrier Head of Legal, and the divestment was closed on June 1st, 2021.

Between the hand-over and the closing of the divestment, Telia Company continued to apply its Policy on Freedom of Expression and Surveillance Privacy, as well as the Telia Company Supplier Code of Conduct, which underscores commitments to developing products, services, and processes that respect individuals' privacy and freedom of expression, to the Telia Carrier operations.

As part of the handover, Telia Company assessed the ethical and human rights standards of the acquiring company and its owners. A key risk identified was that the divested entity would have to build up systems and processes of its own to continue working on sustainability post-sale. To mitigate this, the handover included policies and projects to support continued work within the divested entity.

This case demonstrates how a company can use due diligence processes in the context of a sale/divestment to assess the buyer's ethical and human rights standards and support their development pre and post-sale. In so doing, the company took proactive steps to ensure that privacy and freedom of expression would continue to be core values after the divestment.

Responding to “access disabling” orders in Singapore

Between February and May 2020, Meta (then Facebook) received three “access disabling orders” under Singapore’s Protection from Online Falsehoods and Manipulation Act (POFMA). These orders required the company to block access within Singapore to four pages associated with a self-exiled Singaporean political dissident, Alex Tan.

Meta engaged with the government to express concerns about freedom of expression. Meta applied correction labels, but faced an “access disabling order” for the Page. The company, citing concerns about proportionality, complied under protest.

The case demonstrates how Meta sought to implement GNI implementation guidelines in responding to specific legal changes in Singapore, demonstrating adaptability in response to novel challenges.

A product transformation due to unintended data transfer

Through its Sensitive Business processes, Ericsson discovered that a product had been used in an unintended way in some implementations, impacting users’ privacy. This concerned a key product which is crucial for the future evolution in 5G and IoT. After analyzing the situation within the Sensitive Business process, Ericsson found that the product had been used in unintended ways in some deployments.

Ericsson determined that an earlier version of the product could be used as an enabler for geographic positioning data that could be shared with authorities, despite the fact that this was not what the product was intended to be used for. As a response to these findings, Ericsson developed a new product with a new architecture that prevents it from being used in the identified and unintended way.

This case showed how the GNI framework has been integrated into Ericsson’s policies and practices and how those allowed the company to identify and address potential misuse of their product. It also showed how the Sensitive Business process can allow Ericsson to reshape product solutions to mitigate potential human rights risks.

ANONYMIZED

Responding to legal developments in Pakistan

In November 2020, Pakistan Prime Minister Imran Khan granted the Pakistan Telecommunication Authority the power to remove and block digital content that "harms, intimidates or excites disaffection" toward the government or in other ways hurts the "integrity, security, and defense of Pakistan."

These blanket powers of censorship violated established human rights of privacy and freedom of expression. Additionally, tech companies that did not comply with the removal or block of unlawful content from their platforms within 24 hours could face a fine of up to $3.14M USD.

In response to the new rules, tech companies - including some GNI members - issued a statement expressing deep concern about the new rules, and noting - through the Asia Internet Coalition (a regional industry association) - that "the rules as currently written would make it extremely difficult for AIC Members to make their services available to Pakistani users and businesses."

This case illustrates how companies sought to mitigate the impacts of a new legal development on freedom of expression and privacy, consistent with the GNI framework. Given the increase of such developments across the globe/region, including Vietnam's cybersecurity law passed in 2018, this approach in the face of rules that violate the GNI Principles is an important step in respecting human rights.

yahoo!

Shutdown of Yahoo content in India

In September 2019, the Indian government announced a 26% cap on foreign direct investment (FDI) in digital media. The announcement lacked clarity, but it coincided with several other political developments, such as mandatory registration for digital news providers and proposed amendments to the IT ACT, that caused concern for the impact on freedom of expression. Due to these developments and other factors, Yahoo decided to shut down all content in India at the end of August 2021.

Yahoo's public policy team is responsible for notifying BHRP of potential emerging threats to human rights and the GNI principles. Once an issue is identified, the BHRP works with the policy and legal teams to advise on possible advocacy strategies.

In accordance with these policies, the public policy lead for APAC initially alerted the BHRP team about concerns with regard to emerging policy developments and their potential impact on freedom of expression in India in January 2020. Final guidance on the FDI caps was issued later in October and Yahoo sought an official exemption the following month. Additionally, the company began extensive outreach efforts to the Indian government to seek explicit approval to continue operations above the 26% threshold. After the outreach proved inconclusive, Yahoo had to remove all digital media content, as necessary under the new FDI cap. Once this decision was made, the new Yahoo BHRP team reached out to GNI and the Bureau of Democracy, Human Rights & Labor in the U.S. State Department to update them on the decision and the impact on human rights.

This case illustrates how Yahoo's internal processes worked to identify challenging developments and helped bring relevant internal teams