GLOBAL NETWORK INITIATIVE

Case Studies from the Fourth GNI Assessment Cycle

SUPPLEMENT TO THE 2021/2022 PUBLIC ASSESSMENT REPORT

Table of Contents

Introduction

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.

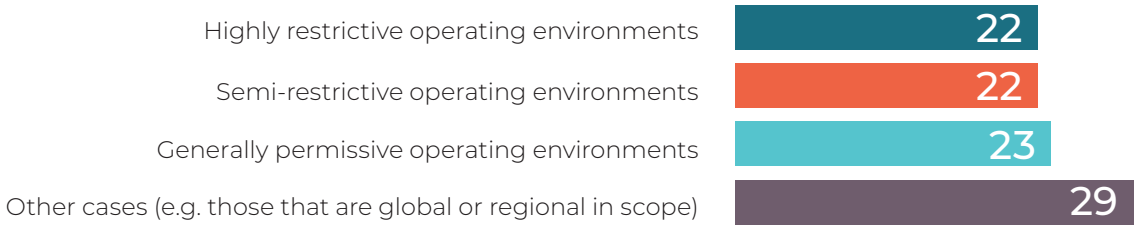
Just as the cases selected for inclusion in each assessment report are not a statistical sample of the thousands of government demands that GNI member companies receive, the cases in this supplement are not necessarily representative of the cases included in this cycle overall, since many of the most 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:

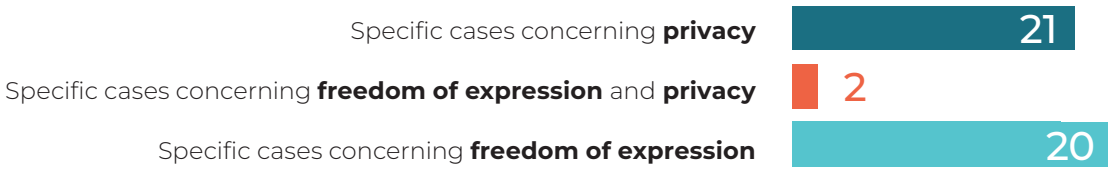
- **Covid-19:** The types of government requests companies faced during the Covid-19 pandemic and how they responded through policy and process.
- **Regulatory pressure:** Increasing regulatory pressures on companies through a range of instruments including licensing regimes, intermediary liability rules, 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

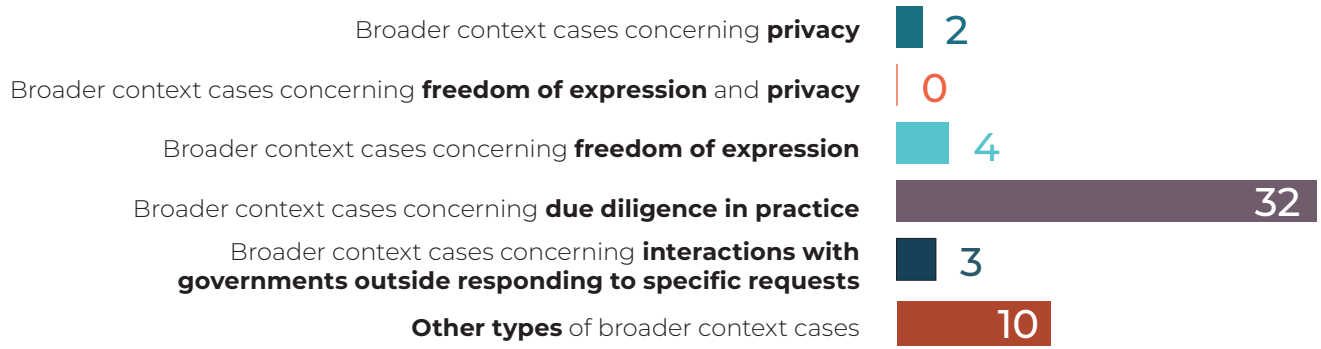
CASES BY OPERATING ENVIRONMENT



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.

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.

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