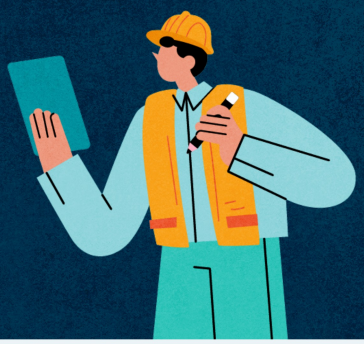
Accountability



Overview

GNI maintains a detailed, multistakeholder-designed framework aimed at advancing freedom of expression and privacy across the tech sector. Central to this effort is GNI's independent assessment process, which is now in its fifth cycle.

GNI's assessment process involves accredited, independent, third-party assessor review of corporate policies, systems, and decision-making frameworks, accompanied by case studies demonstrating real-life implementation. Findings are compiled into confidential reports which are reviewed by the GNI Accountability Committee and the GNI Board to determine whether member companies are implementing the GNI Principles (and their accompanying Implementation Guidelines) in good faith with improvement over time. Companies are also provided with recommendations to better implement the GNI Principles. Technical details of the assessment process are set out in the fifth cycle Assessment Toolkit.



Calendar year 2025 Assessments

Verizon, MTN, Wikimedia Foundation, Google, Meta, and Zoom completed both their Accountability Committee and GNI Board Assessment Review Meetings in 2025. Due to the staggered nature of the fifth cycle assessment process, Cloudflare, Ericsson, Microsoft, Nokia, Orange, Telenor, and Yahoo, who began their assessments during calendar year 2025, are scheduled to complete those assessments in 2026. A summary of their Process Review and Case Studies will be included within GNI's 2026 Annual Report.

Accommodations in the Assessment

From time to time the GNI Board makes adjustments and accommodations to GNI's assessment process. In 2024, the GNI Board permitted Frontiir, an ISP operating exclusively in Myanmar, to engage an independent consultant to conduct an "abridged assessment" due to unique operational and economic challenges related to the ongoing conflict in Myanmar. That abridged assessment began in 2025 and will be completed in 2026, with a summary to be included in GNI's 2026 Annual Report.

Preparations for the Sixth Assessment Cycle

GNI continuously evolves its assessment process between cycles to remain effective amid shifting political, technological, and membership landscapes. Preparations for the sixth cycle began in October 2025 with the Board's approval of a strategic, phased workplan targeted for completion by the end of 2026. This phased approach involves gathering multistakeholder feedback, refining improvements through consultation with the Accountability Committee, membership, and accredited assessors to maximize value for members. Further details on the evolution process and final design of the sixth cycle will be provided next year and summarized in GNI's 2026 Annual Report.



Fifth cycle assessments

The fifth assessment cycle introduced substantial structural and methodological changes, as highlighted by a GNI Confluence Blog from August 2024.

The five key changes are highlighted below:

1. **Incorporating Mandatory Due Diligence Regulations:** Companies and assessors can now use evidence from mandatory human rights frameworks like the DSA, Corporate Sustainability Reporting Directive (CSRD), and Corporate Sustainability Due Diligence Directive (CSDDD) during assessments. (See August 2024 GNI Confluence Blog.)

2. **Enhanced Participation and Improved Mechanics:** GNI's Accountability Committee, composed of a broader range of representative members, now conducts reviews and submits determinations and recommendations to the Board, while the assessment process was staggered into three tranches over a two-year cycle. (See January 2025 Confluence Blog.)

3. **Sector-Specific Tailoring:** Explicit guidance was provided to help assessors evaluate relevant government restrictions and demands based on specific technical capabilities and business models. (See September 2024 Confluence Blog.)

4. **Addressing New Trends in Platform Governance and Information Integrity:** The fifth assessment process better accounts for the increased sophistication of government restrictions, thereby ensuring assessments remain relevant in an evolving digital landscape. (See December 2024 Confluence Blog.)

5. **Government Demands on AI and Due Diligence:** Assessors were equipped to assess how companies conduct due diligence on AI-enabled products and features in light of corresponding government restrictions, further detailed in the GNI Policy Brief on Government Interventions in AI, launched in October 2025.

Accountability Annex:
Public Assessment Reports

Cross-company comparisons

Six companies - Verizon, MTN, Wikimedia, Google, Meta, and Zoom - successfully completed their assessments within 2025. Below is a cross-company analysis, with company-specific detailed summaries included in the Annex.

INTERVIEWS

100 people interviewed across 6 companies – both HQ and regional staff



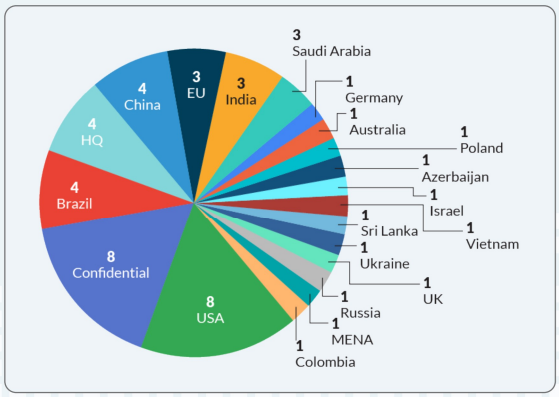
CASE STUDIES

48 cases in total
(8 per company)



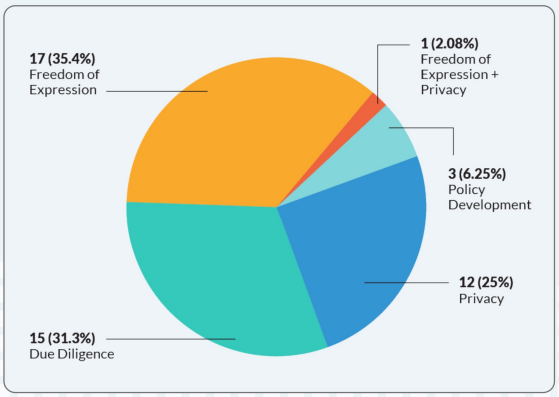
CASE COUNTRIES

25 unique countries / regions covered



CASE CONTENT

Distribution of cases by content



Verizon Company Process Review

ABOUT THE COMPANY

Verizon provides communications, technology, information, and entertainment services to consumers, businesses, and governmental entities. The company's two primary business units are Verizon Consumer Group (VCG) and Verizon Business Group (VBG). Its customers include individual wireless and wireline consumers in the United States and multinational enterprises across approximately 150 countries.

GOVERNANCE

Verizon's governance with respect to potential risks to freedom of expression and privacy includes oversight by the company's Board of Directors. Specifically, the Corporate Governance and Policy Committee of Verizon's Board of Directors has oversight responsibility with respect to human rights and public policy matters. The Audit Committee of the Board has primary responsibility for overseeing Verizon's risk management programs relating to data protection, privacy, and cybersecurity.

Verizon's implementation of the GNI Principles and its overall human rights commitments is conducted primarily through the work of the Business & Human Rights Program (BHRP), a dedicated team of human rights attorneys, operating under the remit of the company's Chief Legal Officer. The company's Human Rights Statement sets forth the company's commitment to assessing the impacts of its activities on human rights in a manner guided by the human rights due diligence framework set forth in the UN Guiding Principles on Business and Human Rights. Regular training and information-sharing briefings are provided to employees to support Verizon's efforts to operate consistently with its human rights commitments.

Development and implementation of policies relating to privacy are the responsibility of Verizon's Privacy Office, under the remit of the Chief Privacy Officer. Day-to-day interaction with law enforcement is managed by Verizon's Security Assistance Team (VSAT) under the Corporate Security organization, with support provided by the law enforcement legal team, which reports up to the Chief Privacy Officer. Training programs include annual mandatory privacy training for all employees, specialized training for personnel with access to customer data, and a four-week training program for new VSAT employees.

DUE DILIGENCE AND RISK MANAGEMENT

Verizon integrates human rights considerations, including potential risks to privacy and freedom of expression, into its corporate decision-making and due diligence frameworks. The BHRP works together with other internal teams, including Privacy, Law Enforcement, Responsible AI, and Third Party Risk Management to assess and address potential human rights risks. In product

development, Verizon utilizes product intake forms and privacy impact assessments to evaluate potential human risks including those related to data collection, user-generated content, and other product or service features that may potentially generate risks to privacy or freedom of expression. Verizon also conducts Human Rights Impact Assessments (HRIAs) in specific instances to assess potential human rights impacts potentially associated with its products and services.

Verizon's efforts to mitigate human rights risks associated with the sale of its products and services may include: modifications to product or service features; the use of acceptable use policies; guidelines around specific technologies, including the deployment of artificial intelligence; and tailored training for relevant employees.

Within the supply chain, the Third Party Risk Management office conducts screenings of new and existing vendors, escalating identified concerns for review by relevant internal teams.

FREEDOM OF EXPRESSION & PRIVACY

Verizon's framework for managing law enforcement demands is governed by a multi-layered corporate structure. Absent an emergency situation, Verizon requires government demands to be made in writing and to be based on appropriate legal authority. Trained analysts confirm the facial validity of each legal demand received. In the United States, the company maintains an emergency demand process where specific protocols are followed to ensure that the legal requirements for disclosing information in an emergency have been satisfied and documentation can be provided retrospectively by law enforcement.

Data privacy is overseen by the Privacy Office. Consistent with U.S. privacy law and its own Privacy policies, Verizon only collects from customers the information the company needs to render and improve the services it provides. Records are retained for as long as they are needed for operational, legal, tax, audit, investigative, and security purposes. Retention practices are reviewed and benchmarked on a regular basis and when new circumstances warrant their review. Verizon informs its customers about the types of data that are collected and the ways in which the data are used and shared. Data security is overseen by the Chief Information Security Officer. Data safeguarding measures used for a particular set of data can vary, but may include encryption, storage on secure servers, and restricting access to a limited number of employees. Data privacy and protection practices are subject to several internal audits each year.

For its international enterprise operations, Verizon uses Binding Corporate Rules (BCRs) to protect the transfer of EU- and UK-originating personal data to participating Verizon entities, approved by applicable regulators. The processing of personal data that is not subject to EU/UK requirements is reviewed and monitored for compliance with applicable law(s) by relevant legal and regulatory teams, including the Privacy Office.

TRANSPARENCY & ENGAGEMENT

Verizon maintains human rights governance disclosures, including its Human Rights Statement and HRIA summaries, on a dedicated section of its corporate website. The company's Human Rights Statement and its Code of Conduct reference respect for internationally recognized human rights. Information regarding Verizon's responses to law enforcement requests in both the United States and in other countries where Verizon does business is available in the company's publicly available Transparency Reports, which have been published since 2013. The reports include information about the applicable laws and regulations that require Verizon to disclose information or to block content.

Verizon has not received demands to block access to websites in the United States, or to shut down or restrict access to its services or communications networks in the United States or internationally. An FAQ in Verizon's Transparency Report states that, if such a request were received, the company would evaluate its legality and proportionality and strive to minimize any impact on customers' freedom of expression and human rights.

Outside of the United States, where Verizon provides network services to enterprise customers, Verizon is, on occasion, required to block access to specified websites, and the company includes these demands in its Transparency Reports.

Information regarding Verizon's Privacy Policies is available in Verizon's online privacy center. Verizon also hosts a dedicated Privacy Dashboard where U.S. consumers can exercise privacy rights.

Grievance mechanisms include a 24/7 multilingual ethics reporting platform accessible to employees, suppliers, and the public. Verizon also has several channels available for customers to raise concerns specifically relating to privacy. For example, customers of Verizon's various consumer brands are provided with contact information to address questions or concerns.
The company engages in multiple external forums related to privacy and freedom of expression, including RightsCon and the B-Tech Community of Practice.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative.

The assessor noted that Verizon's approach to human rights governance reflects maturity, with human rights reviews integrated into core business processes such as product development, partnerships, and legal reviews. Several potential improvement areas were identified by the assessors and/or the GNI Board and Accountability Committee, including: more systematic training for relevant teams; more structured human rights reviews with respect to sales involving

higher-risk products and markets; additional transparency with respect to the policies and guidelines governing responses to law enforcement demands; and integrating human rights perspectives into public policy engagement through greater cross-functional collaboration.

MTN Company Process Review

ABOUT THE COMPANY

MTN Group serves 307.2 million customers across 16 markets in Africa and the Middle East [1]. The Group generates revenue primarily through mobile telecommunications services, including network, digital, fintech, interconnect, and roaming services, and the sale of mobile devices, as well as enterprise, wholesale, and Application Programming Interface (API) solutions. The Group's operations are organized into reportable segments based on geography and reporting lines to the chief operating decision maker, specifically covering South Africa, Nigeria, South and East Africa (SEA), West and Central Africa (WECA), and Middle East and North Africa (MENA).

GOVERNANCE

MTN Group's governance framework for sustainability and digital human rights is overseen by the Social, Ethics and Sustainability Committee (SESCO) on behalf of the Board. The Group Executive Committee, led by the Chief Executive Officer (CEO), is responsible for continuous monitoring, while Country CEOs are accountable for implementing the Digital Human Rights Policy and conducting human rights due diligence within their respective Operating Companies (OpCos). The Digital Human Rights and Data Protection Policies are reviewed biennially and require formal approval from SESCO and the Audit Committee, followed by final Board ratification.

The Group Sustainability function is responsible for policy development and the localization of GNI Principles, while the Executive Committee manages risk mitigation. Implementation at the OpCo level is supported by designated human rights personnel and annual Human Rights Impact Assessments (HRIAs). A Digital Human Rights Playbook ("Playbook") establishes a decision matrix for risk categorization and escalation, specifically addressing government requests for network shutdowns or user data. High and very high-level risks necessitate escalation to the Group level via established crisis management procedures.

The Group maintains a structured training program, facilitated annually by the Group Human Rights Senior Manager, covering human rights frameworks, due diligence, and Playbook navigation. This extends to the MTN Board and includes specialized training for privacy champions. The privacy program comprises extensive documentation and modules designed to ensure regulatory compliance. While OpCos may localize policies to meet regional regulatory requirements, they must adhere to a minimum global standard for data protection. In incident-

related crises, the Group mandates an audit trail, utilizing email communications for immediate record-keeping, followed by formal documentation in accordance with the Playbook.

DUE DILIGENCE AND RISK MANAGEMENT

MTN's due diligence framework for human rights risk management encompasses products, OpCos, and business relationships. At the Group level, technical risks regarding product development, including fintech and Artificial Intelligence (AI), are identified through collaboration between Group Tech, Sustainability, and Legal teams. For geographic operations, OpCos execute annual HRIAs and quarterly risk assessments, supplemented by bi-monthly reviews and biennial third-party audits as prescribed by the Playbook. Heightened assessment protocols are activated during periods of political instability or elections to mitigate risks to freedom of expression and privacy.

In high-risk or conflict-affected environments, the company utilizes rapid impact assessments to address isolated incidents, such as Internet shutdowns. For acquisitions, policy mandates a completed impact assessment prior to the acquisition of new business to ensure human rights protections are maintained. While Group Procurement currently manages supplier due diligence concerning labor practices, the integration of digital human rights principles into this process is ongoing, utilizing a toolkit aligned with the UN Guiding Principles on Business and Human Rights and other international frameworks.

To manage government-mandated service restrictions, MTN conducts regulatory engagement and collective industry action. Identified human rights risks and mitigation recommendations are reported to the SESCO, the Board, and Group Risk to ensure oversight and continued policy integration.

FREEDOM OF EXPRESSION & PRIVACY

Under the guidance of the Sustainability & Shared Value Department, all government requests for content restrictions or data are evaluated for legal validity, necessity, and proportionality. While the company maintains compliance with domestic laws, international human rights standards serve as the overarching framework in instances where domestic legislation conflicts with international norms. Requests concerning freedom of expression and data privacy are processed at the OpCo level, with legal teams performing the primary assessment and sign-off.

Procedural deviations from the requirement for written communication are documented, particularly in conflict-affected regions where verbal instructions are recorded and escalated to the Board. In some markets, OpCos have implemented a requirement that all requests be channeled through the national regulator to ensure formal documentation. Data privacy is further managed via a Group Data Protection Policy and an initiative involving the appointment of departmental "privacy champions" and mandatory staff training.

TRANSPARENCY & ENGAGEMENT

MTN utilizes several formal communication channels, including an annual Sustainability Report, biennial Position Statements, and Group Statements in case of urgent matters. Internally, the company conducts annual Digital Human Rights training for specified OpCo teams, including Legal and Corporate Affairs. Regarding data privacy, the company discloses the categories of personal information collected, while incident management for privacy or digital human rights violations is handled via a collaborative process between Group and OpCo Cyber and Information Security (Infosec) teams.

In response to government-mandated content restrictions or data requests, MTN generally notifies users via Short Message Service (SMS); however, disclosures may be delayed depending on the legal context and the nature of the incident. In certain markets, the company has encountered government instructions to withhold communication regarding network disruptions.

The company maintains grievance mechanisms, including a dedicated human rights email address and a 'Treat Customers Fairly' policy, with remediation measures such as the provision of free minutes. Stakeholder engagement is primarily conducted through discussions surrounding operating licenses and investments, and MTN liaises with international bodies and governments regarding human rights infringements on a case-by-case basis.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative.

The assessor appreciated MTN's foundational commitment to digital human rights, specifically noting the value of its Digital Human Rights Playbook and active industry collaboration. These elements provided a solid framework for responsible business practice, though the assessor noted that enhancing their practical application is essential for sustained compliance.

The assessor recommended localizing and simplifying the Playbook to ensure accessibility for non-expert staff at OpCos. Furthermore, the assessor noted that streamlining due diligence by integrating human rights assessments into lateral business functions — such as Mergers and Acquisitions (M&A) and product development — would ensure a more proactive risk management posture. Finally, the assessor identified a need for formalized record-keeping regarding government requests and post-incident management. The assessor concluded that by expanding technical training and increasing transparency through published HRIA summaries, MTN can more effectively align its reporting standards with GNI guidelines to strengthen accountability. The GNI Accountability Committee and Board took note of and supported these recommendations.

[1] In Nov 2025, MTN streamlined its operating model for greater efficiency and growth. As a result our operations are organized as follows: South Africa; Nigeria; SEA (Southern and East Africa) and Francophone Africa]- for more info please see page 8, MTN-Group-FY-25-Integrated-Report-v1.pdf

Wikimedia Foundation Company Process Review

ABOUT THE COMPANY

The Wikimedia Foundation (the Foundation) is the non-profit organization responsible for operating Wikipedia and other free knowledge projects globally. Funding is primarily sourced from individual donations. The Foundation fulfills the technical, legal, trust & safety, administrative, fundraising, and other functions necessary to host these projects, while the projects and the content they host are moderated through a decentralized, community-governed model. The organization includes a for-profit subsidiary, Wikimedia Enterprise, which provides services to high-volume commercial re-users of Wikimedia content.

GOVERNANCE

The Foundation has integrated human rights protections into its senior management structure through a cross-functional Human Rights Steering Committee. This committee, which is composed of representatives from the Legal, Global Advocacy, Communications, People, and Product and Technology teams, is responsible for implementing the Foundation's Human Rights Policy and the GNI Principles. Oversight is maintained by the Board of Trustees via the Executive Committee, which receives regular reports on human rights trends. The Board includes at least one member with human rights expertise, and a community-led governance structure facilitates the escalation of volunteer concerns to the Foundation's senior management. Operational implementation of privacy and freedom of expression is distributed across the Privacy, Product and Technology, Trust and Safety, and Human Rights teams.

The Foundation provides various privacy-related trainings, such as training for new employees on general privacy practices, as well as training for relevant staff to address data breaches. Formal reporting mechanisms are established for specific risk categories: legal threats are routed to the Legal Department, on-platform issues such as harassment are managed by Trust and Safety through a multilayered review and appeal process, and physical safety emergencies are addressed via a 24/7 monitored email that may trigger a crisis response protocol. Furthermore, a Whistleblower Policy allows internal stakeholders to report potential legal or ethical violations through leadership or an anonymous hotline, with oversight provided by the Chair of the Audit Committee.

DUE DILIGENCE AND RISK MANAGEMENT

The Foundation employs an institutionalized human rights due diligence (HRDD) framework to identify and mitigate risks to freedom of expression and privacy. This framework informs decision-making regarding new product development, significant changes to existing products, and ad hoc events such as armed conflict. Risks are classified as high, medium, or low. High-risk scenarios in conflict-affected areas may trigger rapid assessments, while medium-risk scenarios may result in

product or country-level impact assessments. Assessment methodologies incorporate internal policies, consultations with staff and volunteers, and external academic or civil society research, such as Freedom House reports.

To evaluate risks that emerge in specific jurisdictions, the Legal Department reviews domestic laws and practices against international human rights norms. Regarding business relationships, the Foundation's Legal, Safety, and Security Service Center (L3SC) serves as a centralized intake for evaluating commercial partnerships and assessing potential risks. For risks within the Foundation's operational control, such as government content removal or data requests, a dedicated legal team conducts rigorous reviews of each request. For risks where the Foundation lacks operational control, such as state-level platform blockages, the Foundation may consider legal challenges through relevant judicial bodies.

The Foundation's governance structure ensures that findings from Human Rights Impact Assessments (HRIAs) are escalated from the Human Rights Steering Committee to Senior Leadership and the Board of Trustees. These findings may be institutionalized through policy updates, the creation of specialized roles, and the integration of recommendations into annual budget and resource planning processes.

FREEDOM OF EXPRESSION & PRIVACY

The Foundation's privacy and litigation functions are responsible for designing, implementing, and revising all policies for responding to government demands concerning freedom of expression and privacy. The Foundation's policies that govern how it responds to such demands mandate that all government requests for user information or content alteration or removal be legally valid, enforceable under applicable law, submitted in writing, and necessary and proportionate. Any request that fails to adhere to these procedures or lacks a valid legal basis is refused, except in situations involving an imminent threat to life. For requests from governments, the Foundation applies its policy to determine the applicability of a jurisdiction's law to the organization, which ensures compliance with international human rights norms. To further mitigate risks, the Foundation adheres to strict data minimization principles by collecting minimal amounts of personal data and retaining the data it does collect for a minimal period of time. Detailed records of all incoming government requests are maintained to ensure accountability.

TRANSPARENCY & ENGAGEMENT

The Foundation ensures transparency through a biannual Transparency Report that summarizes requests for content alteration and removal and user information. The Foundation's Privacy Policy discloses the categories of personal information collected and their specific uses, and the Foundation aims to notify users within ten days of information sharing, where feasible. While the vast majority of content moderation is managed via community self-governance,

any Foundation-led removals following valid legal orders are recorded publicly in platform edit histories and the Transparency Report. Stakeholders may submit grievances and seek redress through the Foundation's Legal Department or through mechanisms described in the Foundation's Whistleblower Policy.

The Foundation also engages in substantive public policy advocacy and litigation to protect users' rights. This includes challenging the constitutionality of the United States' National Security Agency (NSA) mass surveillance program and opposing policies including the French SREN (Law to Secure and Regulate the Digital Space) bill, Chilean regulations that threatened community-led moderation, and the Philippines' SIM Card Registration Act, while advocating for the reform of Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) and contributing to discussions regarding Australia's Basic Online Safety Expectations.

RECOMMENDATIONS

This section provides summaries of some of the recommendations made to the company through the assessment process. It is not comprehensive or illustrative.

The assessor noted that while the Foundation successfully relies upon its decentralized model to uphold GNI Principles, implementing standardized, documented protocols is essential for consistency when responding to government demands across jurisdictions. Recommended improvements include formalizing mandatory human rights training for staff, establishing clear timelines for implementing HRIA recommendations, and clarifying when community consultation is required to more proactively mitigate risks.

GNI's Board and Accountability Committee further recommended that the Foundation implement recurring, region-specific human rights and digital security training for community members and volunteers, developed in collaboration with civil society organizations. To better protect global stakeholders, they also recommended deepening engagement with civil society, bolstering security measures to safeguard contributor data, and increasing transparency regarding content blocking orders in conflict-affected areas in accordance with applicable laws.

Google Company Process Review

ABOUT THE COMPANY

Google, a subsidiary of Alphabet Inc., is headquartered in Mountain View, California, and maintains 116 global offices. The company's operations include core platforms such as Search, Android, and YouTube—each exceeding one billion monthly active users—alongside enterprise cloud and hardware businesses. Following structural reorganizations, DeepMind now operates as Google DeepMind. The company's mission to organize global information is conducted in accordance with international human rights standards.

GOVERNANCE

Google has integrated its Human Rights Executive Council (HREC) into a formalized risk and compliance governance structure. The HREC is composed of senior leaders across relevant product areas and functions. The Council is formally integrated into Google's Trust and Compliance governance program, which is led by the Trust & Compliance Council (TCC). The TCC is co-chaired by Google's President of Global Affairs & Chief Legal Officer and SVP of Core Engineering. The HREC provides oversight and guidance across Google's human rights efforts and ensures issues are being addressed consistently. 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 Human Rights Team operates under the President of Global Affairs, with day-to-day oversight distributed among the Vice Presidents of Global Government Affairs and Public Policy, Trust & Safety, Regulatory Affairs, General Counsel, and Chief Compliance Officer. This structure ensures that critical functions, such as content removal and user data requests, are managed by teams trained to identify potential infringements on freedom of expression and privacy. To support this, Google provides training for all personnel on identifying and escalating human rights risks, supplemented by specialized GNI training for core teams. Furthermore, an anonymous, retaliation-protected reporting hotline facilitates the internal identification and escalation of human rights concerns.

DUE DILIGENCE AND RISK MANAGEMENT

Google maintains a structured due diligence framework to identify and mitigate risks to freedom of expression and privacy across its global operations. During the product development lifecycle, product-specific counsel and cross-functional review bodies assess potential impacts on user rights. For jurisdictional expansions or changes, regional legal and public policy teams, in

coordination with the Human Rights Team, evaluate local legal and political environments. In high-risk or conflict-affected scenarios, the company establishes centralized, cross-functional teams guided by standardized playbooks. Acquisitions and partnerships are subjected to rigorous legal and privacy due diligence to ensure contractual adherence to company principles.

Google conducts 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. For novel or high-impact issues, Google may conduct formalized Human Rights Impact Assessments (HRIAs), often utilizing third-party experts and international standards such as the United Nations Guiding Principles on Business and Human Rights (UNGPs).

FREEDOM OF EXPRESSION & PRIVACY

Policy design and oversight regarding government demands are managed by the Data Disclosure & Strategy team and the Legal Content Policy & Standards (LCPS) team within Global Affairs. Google requires that all government requests for user information or content removal adhere to established domestic legal processes and be submitted through written, substantiated communications via official government email addresses. The company reviews the legal validity of each request, assessing the authority of the issuing entity and the application of local laws. If a request is vague, ambiguous, or lacks sufficient legal basis, Google may push back or deny the request.

To promote global digital freedoms, Google engages with international organizations, including the Organisation for Economic Co-operation and Development (OECD) and the UN, to advocate for standards and regulations consistent with international human rights laws. Regarding data privacy, Google takes a privacy-by-design approach, adheres to data minimization principles, and maintains clear policies for data retention and deletion. Furthermore, Google conducts jurisdiction-specific risk assessments to determine data storage locations, utilizing encryption and stringent internal access controls to mitigate risks associated with varying jurisdictional footprints.

TRANSPARENCY & ENGAGEMENT

GGoogle maintains transparency regarding human rights impacts through its online Transparency Reporting portal, which contains a series of reports including on government requests for user data and to remove content. This is supplemented by product-specific policies, a dedicated human rights webpage, a Safety Center, and a detailed Privacy Policy. Upon content removal due to government mandates, Google's standard practice is to notify affected users via email or on-page notices, unless prohibited by court orders; these removals are also shared with the Lumen database. Users may appeal content removals through a process reviewed by human personnel.

Externally, Google regularly meets with NGOs, human rights organizations, international organizations, and regulators to discuss human rights issues. Additionally, the company participates in spaces like the Freedom Online Coalition, Internet Governance Forum, and interacts with the UN High Commissioner for Human Rights. 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 Team, in collaboration with various teams, including Legal, Regulatory Affairs, Trust & Safety, and Compliance.

FOLLOW UP & IMPROVEMENT

The assessor noted that Google maintains a sophisticated framework for respecting user privacy and freedom of expression, demonstrating rigor in assessing government requests and responsible AI development. To further strengthen the implementation of the GNI Principles, the assessor recommended scaling regional human rights capacity across the Asia-Pacific (APAC), Latin America (LATAM), MENA, and Sub-Saharan Africa (SSA) markets to ensure more nuanced, context-aware responses. Additionally, recommendations were made by the assessor to increase public transparency regarding specific human rights interventions and sustain investment in generative AI governance to ensure protocols remain robust as technology evolves.

RECOMMENDATIONS FROM PREVIOUS CYCLES

Since the 2022 assessment, the assessor noted that Google has implemented most recommendations regarding governance, capacity, and crisis readiness. The Human Rights Program governance is now formally integrated into the broader companywide compliance infrastructure, and the Human Rights team has expanded, enabling increased stakeholder engagement via regional engagements. Google has also established a protocol related to human rights & crisis response. The assessor identified ongoing opportunities to improve public transparency and to further embed human rights considerations into high-level internal forums.

Meta Company Process Review

ABOUT THE COMPANY

Meta's primary products relevant to the Global Network Initiative (GNI) are Facebook, Instagram, Threads, Messenger, WhatsApp, and Meta AI. According to its December 2024 10-K filing, Meta reported 3.35 billion daily active users across its products.

GOVERNANCE

Meta's approach to human rights is governed by its Corporate Human Rights Policy (CHRP), which incorporates its commitment to the GNI Principles. Implementation of Meta's CHRP is jointly overseen by the President of Global Affairs and Chief Legal Officer.

Meta's Human Rights Program is responsible for day-to-day human rights risk management. The Human Rights Program advises on key product, policy, and corporate decisions; and leads human rights due diligence efforts. The team works closely with Legal, Operations, Policy, and Product leadership and staff to ensure Meta lives up to the expectations of the UN Guiding Principles on Business and Human Rights (UNGPs) as well as its commitments as a member of the Global Network Initiative.

Significant and challenging matters may be escalated to the President for Global Affairs, Chief Legal Officer, and other relevant senior leadership, as appropriate.

DUE DILIGENCE AND RISK MANAGEMENT

Meta's Corporate Human Rights Policy lays out its approach to conducting due diligence and managing human rights risks in a manner aligned with the UNGPs and GNI Principles. The company employs a variety of due diligence methodologies, including, but not limited to, human rights impact assessments (HRIAs), to assess potential human rights impacts of its products and business activities. It endeavors to pay particular attention to the rights and needs of users from groups or populations that may be at heightened risk of becoming vulnerable or marginalized.

As part of its due diligence program, Meta periodically carries out a review to identify and prioritise its most salient human rights issues in each context using the UNGP's framework of severity (scope, scale, remediability) and likelihood; it first disclosed a summary of these salient risks in its 2022 Human Rights Report. In managing dynamic country-specific risks—including those related to elections and conflict-affected environments—Meta synthesizes internal data, external sources, and findings from its comprehensive stakeholder engagement program. It also considers its relevant legal obligations and the safety of its personnel in the jurisdictions where it operates.

FREEDOM OF EXPRESSION & PRIVACY

Meta has established policies and processes for reviewing and responding to government requests to disclose user data and restrict content. These include its Law Enforcement Guidelines and Privacy Policy (for user data) and its policies related to content alleged to violate local law, which are informed by its commitment to the GNI Principles.

When Meta receives government requests to restrict content based on local law, it follows a four-step process described in its Transparency Center. First, it reviews the reported content under its policies, such as its Community Standards. Second, it conducts a legal review of the request against applicable local law. Third, it conducts human rights due diligence, including a consideration of legality, legitimacy, necessity, proportionality, and external risks. Finally, it takes any appropriate action on the content and notifies the requesting government agency of the outcome. When Meta takes action on content based on a legal request, it also considers whether any mitigation measures may be deployed, such as an appeal of the takedown request, real time transparency via a public case study, sending a copy of the order to Lumen, or taking steps to limit the impact of the request.

When Meta does act against organic content on the basis of local law rather than its Community Standards, it restricts access to the content only in the jurisdiction where it is alleged to be unlawful. The poster of the restricted content and any attempted viewers impacted by the restriction are informed of the action taken, unless prohibited by law.

When Meta receives a government request to disclose user data, it reviews and evaluates each request individually, whether the request was submitted as related to an emergency or through legal process obtained by law enforcement or national security authorities. This team considers whether requests are consistent with applicable law and Meta's policies (including its Data Policy). In line with Meta's commitments as a member of the Global Network Initiative and its Corporate Human Rights Policy, Meta also conducts a careful review of each law enforcement request to disclose user data for consistency with international human rights standards.

If Meta determines that a government request is not consistent with applicable law or its policies, it will push back and engage the governmental agency to address any apparent deficiencies. If the request is unlawful (for example, overly broad, or legally deficient in any way), it will challenge or reject the request.

Meta notifies users about requests for their information before disclosing it unless it is prohibited by law from doing so or in exceptional circumstances, such as where a child is at risk of harm, emergencies or when notice would be counterproductive. Meta will also provide delayed notice upon expiration of a specific non-disclosure period in a court order and when it has a good faith belief that exceptional circumstances no longer exist and when it is not otherwise prohibited by law from doing so.

In all cases, and consistent with the GNI Principles and Implementation Guidelines, Meta considers the safety of its personnel and impacts on the availability of its services when reviewing government requests.

TRANSPARENCY & ENGAGEMENT

Meta maintains a Transparency Center, where it publishes detailed information on its approach to government requests impacting freedom of expression and privacy as well as jurisdiction-level data on such requests it receives. Through its CHRP, Meta also commits to publishing annual reporting on its human rights work, including work relevant to its implementation of the GNI Principles.

Meta's CHRP includes a commitment to stakeholder engagement, which supports its broader due diligence and risk management activities, described above. The company also engages on salient human rights issues—as appropriate and consistent with the GNI Principles—with governments and international institutions.

FOLLOW UP & IMPROVEMENT

Meta's independent assessor recommended several areas for possible follow-up and improvement. These included periodic retrospective reviews of escalations; increasing the capacity and internal awareness of the company's human rights team; establishing clear criteria for when issues must be evaluated by the human rights team before a decision is made; and more clearly communicating certain rejections of government data disclosure requests to law enforcement.

The GNI Accountability Committee and Board further recommended that Meta deepen employee understanding of geopolitical and conflict-specific context; mandate formal human rights training for relevant members of product teams; and provide further detail in notifications provided to users when their content is restricted or removed based on a government request.

Additionally, in light of concerns raised by some GNI members about its January 2025 product and content policy changes—which occurred outside the assessment period—the Board and Meta also agreed that Meta would make a senior leader involved in the decision-making available for a GNI learning call and would conduct a GNI Case Study Tabletop Exercise (CSTE) exploring the topic. This CSTE will be incorporated into Meta's next GNI assessment.

RECOMMENDATIONS FROM PREVIOUS CYCLES

Meta's independent assessor determined that it had successfully implemented prior recommendations. These included clarifying the role of senior management in human rights decision-making; providing additional human rights training; incorporating human rights considerations into its due diligence on mergers and acquisitions; and establishing more formal processes for conducting human rights due diligence. Meta's assessor also noted that the company had improved stakeholder communication through its annual human rights reporting and clarified its approach to government requests within its Privacy Policy.

Zoom Company Process Review

ABOUT THE COMPANY

Zoom Communications, Inc. was founded in 2011, has been publicly listed since 2019, and provides a workplace collaboration platform. As of April 2025, the company maintains approximately 7500 employees globally, with research and development (R&D) and operational centers in the United States, Europe, China, India, and Singapore. The organizational structure comprises five primary divisions — Product and Engineering, Sales, Finance, Technology, Corporate Strategy — reporting to the Chief Executive Officer (CEO), Eric Yuan.

GOVERNANCE

Zoom's Board of Directors oversees an Executive Staff composed of the CEO and the heads of its primary functions. The Government Relations team and the Trust & Safety Team (which sits within Compliance) have shared responsibility for implementing the GNI Principles. Risks to freedom of expression and privacy are escalated through the management chain where appropriate, to the Executive Staff. Standard Operating Procedures (SOPs) govern the escalation of sensitive issues, such as significant government requests or privacy-impacting product changes, through defined tiers to the Executive Staff or Board. To maintain the SOPs, all employees and senior management undergo annual training on data security and the handling of government requests. Written policies further mandate the reporting of data breaches and require employees to refer sensitive matters to authorized teams.

DUE DILIGENCE AND RISK MANAGEMENT

Zoom employs a multi-layered due diligence framework to manage risks associated with product development, geographic expansion, and third-party relationships. During product development, the company utilizes Privacy Impact Assessments (PIA) for features involving personal data, artificial intelligence (AI), or biometrics, supplemented by Trust & Safety Product Reviews that evaluate features involving encryption and user-generated content. For geographic expansion, Zoom conducts Market Readiness Assessments to evaluate local legal, political, and security risks, supported by a global law enforcement compendium. Third-party risk management is handled by a dedicated team that screens potential acquisitions and business partners for sanctions, export controls, financial viability, and human rights violations.

To mitigate risks during product usage, the Protection and Recovery Team enforces Acceptable Use Guidelines, which include protocols for academic freedom and restrictions on employee authority regarding user bans. While the company has not conducted formal Human Rights Impact Assessments, human rights considerations are integrated into existing PIAs and Market Readiness Assessments. In high-risk jurisdictions, Zoom implements operational restrictions to minimize data

access and advocates against mandates for data localization to protect user privacy and employee safety.

FREEDOM OF EXPRESSION & PRIVACY

Policies regarding freedom of expression and privacy are designed and overseen by the CCO and the Senior Managing Counsel for Law Enforcement Response. All government requests must be submitted in writing through the Law Enforcement Request System (LERS), where the company applies the narrowest possible interpretation to data disclosures. Zoom adheres to strict legal standards, complying with warrants in the United States and Mutual Legal Assistance Treaties (MLATs) or the CLOUD Act internationally. For example, in multiple jurisdictions, analysts limit data provision to users specifically within the requesting jurisdiction unless a formal MLAT or CLOUD Act protocol is followed.

Evidence of rigorous oversight is reflected in Zoom's rejection of legally insufficient requests; between July and December 2024, the company rejected 17% of U.S. orders and over 50% of non-U.S. orders due to invalidity or lack of responsive data. Furthermore, Zoom enforces strict jurisdictional boundaries, such as withholding data from certain, non-democratic authorities except in cases involving child safety or immediate physical harm. To further protect user privacy, the company utilizes role-based access controls, undergoes bi-annual audits, and does not facilitate the interception of meeting content.

TRANSPARENCY & ENGAGEMENT

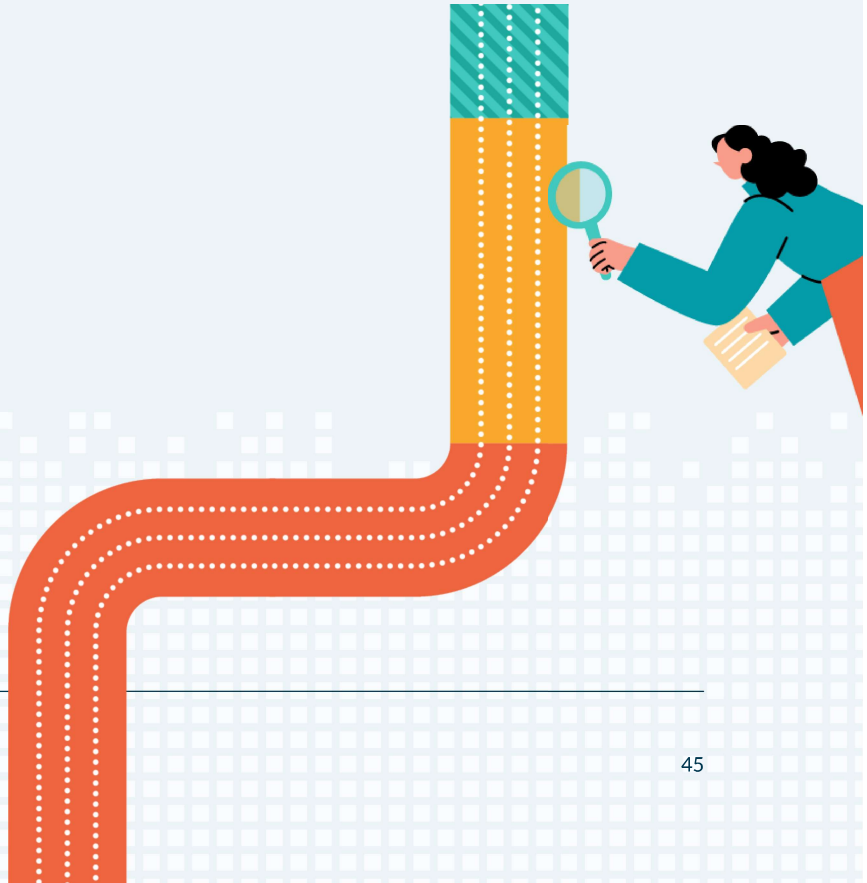
Zoom maintains public-facing disclosures via its "Privacy at Zoom" page and Safety Center, providing documentation on data collection, processing, and retention. Semi-annual transparency reports detail requests from government authorities, and a Government Requests Guide is incorporated into the Terms of Service and Master Subscription Agreement. The company's policy is to notify users of content removal or data disclosures unless legally prohibited or in limited categories of high-risk crimes, and any non-disclosure orders must include a fixed duration.

Externally, the Government Relations Team engages with global authorities to advocate for the rule of law and provides comments on international legislation, such as the Kingdom of Saudi Arabia's draft Personal Data Protection Law. Zoom also participates in the Global Network Initiative (GNI) to support privacy and freedom of expression. Reporting mechanisms are available for users to report security vulnerabilities, violations of Acceptable Use Guidelines or appeal account deactivations, while employees have access to confidential reporting channels through the Code of Business Conduct and Ethics.

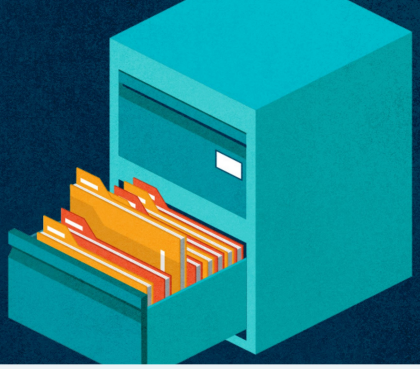
RECOMMENDATIONS

The assessor noted that Zoom has successfully integrated its "Care" value into a robust Compliance and Trust & Safety framework, featuring well-defined escalation processes and systematic government request handling. The assessor also commended the company for formalizing Market Readiness Assessments and strengthening privacy due diligence. However, it was recommended that Zoom establish a senior-directed human rights function and explicitly integrate freedom of expression and privacy considerations into escalated content moderation reviews and partner due diligence. Additionally, Zoom was advised to conduct formal Human Rights Impact Assessments when salient risks are identified and provide Board members with specialized training on the GNI Principles.

The GNI Board and Accountability Committee further recommended that Zoom implement ongoing human rights due diligence and establish clear criteria for conducting formal impact assessments. Finally, they suggested that Zoom expand its internal guidance on responding to overreaching government requests originating outside the United States.



Selected Company **Case Studies**



CASE STUDY:

Development of International Law Enforcement Request Guidelines (Verizon)

Verizon initiated a cross-functional effort to further standardize its response to international law enforcement requests. This initiative was driven by the need to harmonize previously siloed regional processes and was informed by previously developed internal protocols and considerations.

As a result of this cross-functional effort, Verizon developed the "International Law Enforcement Request Guidelines." This framework, overseen by various internal functions, mandates that all requests be assessed for legal validity and processed to minimize impact on privacy and freedom of expression. The guidelines establish rigorous escalation protocols, requiring that requests potentially facilitating human rights violations be escalated for human rights legal review. Furthermore, the company maintains accountability through transparency reporting on the volume of requests received. The implementation involved a coordinated global rollout, including localized contact details and mandatory training for frontline staff globally.

This case illustrates the effective operationalization of high-level human rights principles into core business processes, creating a unified, cross-functional governance structure that proactively identifies, manages, and mitigates human rights risks through standardized policy, training, and oversight.

CASE STUDY:

Brazil Case (Wikimedia)

This case involved the Wikimedia Foundation exploring the establishment of a caching server in Brazil in 2023 to enhance service for users across South America. The initiative aimed to reduce latency, thereby improving access to free knowledge and supporting freedom of expression, particularly for mobile users and marginalized communities. The project was guided

by the Wikimedia Human Rights Policy, the HRDD Framework, and the Human Rights Steering Committee, ensuring that human rights considerations are integrated into organizational decision-making and provide a structured process for escalating findings to senior leadership in line with the GNI Principles. In line with these governance requirements, the Foundation conducted a comprehensive human rights review in line with the GNI Principles to ensure the project aligned with its values and commitments to human rights. To support the operationalization of the server, the Foundation implemented several safeguards intended to preserve user privacy and to promote physical security of the assets. This case illustrates the effective application of a structured governance process to balance technical expansion with the respect for human rights, demonstrating how a proactive due diligence framework enables the Foundation to identify opportunities for increasing knowledge equity while implementing professional safeguards to ensure the continued protection of its global community.

CASE STUDY:

Online Influence Networks (Meta)

In August 2023, Meta announced that it had taken action against two of the largest known cross-internet covert influence networks—one from China (known as Spamouflage) and one from Russia (known as Doppelganger in the security community)—for violating Meta's Coordinated Inauthentic Behavior policy. The company published detailed threat research on both networks in its Q2 2023 Adversarial Threat Report and shared related threat indicators with the broader community.

Acting against the China-based network, which the company investigated after reviewing public reporting about off-platform activity that targeted a human-rights NGO, Meta took down thousands of accounts and Pages that were part of the largest known cross-platform covert influence operation in the world. It targeted more than 50 apps, including Facebook, Instagram, X (formerly Twitter), YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, VKontakte, Vimeo, and dozens of smaller platforms and forums. Meta was able to tie this activity together to confirm it was part of one operation known in the security community as Spamouflage and link it to individuals associated with Chinese law enforcement.

Responding to the Russian network, Meta blocked thousands of malicious website domains as well as attempts to run fake accounts and Pages on its platforms. This operation was focused on mimicking websites of mainstream news outlets and government entities to post fake articles aimed at weakening support for Ukraine. It had now expanded beyond initially targeting France, Germany and Ukraine to also include the US and Israel. At the time, it was the largest and the most aggressively-persistent Russian-origin operation Meta had acted on since 2017.

This case illustrated how Meta considers human rights factors, including potential impacts on freedom of expression, as part of its work to address state-sponsored influence operations, as well as how this work is connected to the company's commitment to protecting human rights defenders using its products.

CASE STUDY:

Controversial Speaker Case (Zoom)

This case involved Zoom blocking meetings featuring a member of an organization designated as a foreign terrorist organization by the U.S. government. Zoom's governance is supported by its Acceptable Use Guidelines, a Tiered Review System, and a corresponding Standard Operating Procedure. For reports concerning potential terrorism or violence, Zoom utilizes a Tier III review process. This involves analysing open-source information and consulting global intelligence teams and multistakeholder initiatives, such as the Global Network Initiative, to reach a good-faith conclusion.

In the specific case, the company's response was based on federal anti-terrorism laws and its terms of service. Zoom also issued an Academic Freedom Statement to refine the enforcement of its guidelines within higher education. Developed in consultation with American universities and the American Association of University Professors, Zoom consults academic institutions before taking action, unless there is an immediate safety threat or significant legal risk.

The case illustrates the application of a structured review process to balance legal compliance with the promotion of academic freedom, integrating collaboration with external experts and internal tiered reviews to ensure a consistent and documented approach to content moderation.

CASE STUDY:

Law Enforcement Request for Customer Records (Verizon)

This case involved Verizon's response to a search warrant issued by a court in Mercer County, Illinois, seeking subscriber information, call detail records, text content, and location records. Verizon's compliance with such requests is governed by its internal Court Order and Warrant Guidelines, which mandate a rigorous review of all law enforcement demands to ensure legal validity, specifically requiring that warrants for customer content records or cell site location information must explicitly state a finding of probable cause.

Verizon's analysts and legal team determined that the warrant was deficient, as it lacked a judicial finding of probable cause. Upon identifying the deficiency, the company notified law enforcement that valid legal process was required. Law enforcement did not modify the warrant, and Verizon received notice that it was in violation of a court order. Verizon subsequently appeared in court to defend its conduct, noting that the warrant did not include a finding of probable cause. The dispute resulted in a judicial directive to modify local warrant templates to ensure that probable cause determinations would be clearly stated going forward. Verizon eventually complied only after receiving a revised warrant that explicitly stated probable cause.

This case illustrates Verizon's active enforcement of domestic legal standards and its commitment to challenging government requests that lack a proper legal basis.

CASE STUDY:

National Identification Registration (Anonymous)

This case involved a telecommunications company operating in a country where the government mandated that all mobile subscriptions be linked to a national identification number to enhance national security. The company's actions were guided by its Digital Rights Policy and Group Digital Human Rights Policy, which emphasize respecting subscribers' privacy and freedom of expression while ensuring that regulatory directives are legally valid and clearly communicated.

The company responded by verifying the legal validity of the government directive and engaging with authorities to secure multiple deadline extensions. To minimize service disruptions, the company implemented a comprehensive communication strategy using television, radio, SMS, and direct staff engagement to notify affected users. From a technical perspective, the company ensured that disconnections were reversible by providing remote self-service verification tools via unstructured supplementary service data (USSD) and web portals. Following a court injunction that barred the deactivation of unlinked lines, the company suspended the barring process and initiated an appeal to resolve the matter.

This case illustrates the application of the GNI Principles where local regulatory requirements conflict with the respect of human rights. It highlights the company's efforts to balance legal compliance and license maintenance with the objective of minimizing impacts on users through proactive communication and technical planning for service restoration.

CASE STUDY:

DSA Case (Google)

This case involved the analysis of the overlap between Google's compliance with the European Union's Digital Services Act (DSA) and its implementation of the GNI Principles. Google uses its established global human rights-based approach and the GNI Principles as guiding frameworks. Its internal governance incorporates a multi-tiered escalation process involving the Trust & Compliance Steering Committee and the Google Ireland Limited board to ensure senior leadership oversight of risk assessments. Google leveraged existing risk assessment processes when it built its DSA systemic risk assessment program. This included classifying systemic risks and calculating inherent and residual risk scores using established methodologies in the fields of fundamental rights and systemic risk assessment. To enhance transparency, Google maintains an online Transparency Center where users can access product policies and reports on removal requests. The company also extended its established grievance mechanisms and lawful request review processes to a broader array of products and services.

The case illustrates the synergy between voluntary human rights commitments and regulatory compliance, demonstrating how leveraging existing frameworks such as the GNI principles, can facilitate the efficient implementation of new legal obligations. Additionally, it shows that regulatory requirements can encourage the expansion of robust governance and transparency standards across a wider range of company services.

CASE STUDY:

Saudi Arabia Case (Anonymous)

This case involved a company's launch of a new product offering in Saudi Arabia, where there were concerns about potential misuse of user data. To manage operational risks, the company utilized its internal processes and escalation structures, which evaluate factors such as human rights, the rule of law, and government surveillance. The company also engaged external human rights consultants to conduct a formalized Human Rights Impact Assessment (HRIA) and aligned its approach with GNI Principles. The company implemented several mitigation strategies, including default data encryption and contractual limits on specific activities. The company also incorporated input from non-governmental organizations to inform its risk considerations.

The case illustrates a structured approach to due diligence when expanding services into new regions with challenging human rights records, integrating technical protections, legal safeguards, internal review committees and stakeholder consultation to respect privacy and freedom of expression.

CASE STUDY:

Law Enforcement Request for Customer Records (Verizon)

The case involved Verizon receiving a search warrant issued by a court in Fresno County, California, requesting records related to a named individual, telephone number, and email address. The records requested included, among other things, call detail records, SMS content, and location records.

Verizon's compliance with such requests is governed by its internal Court Order and Warrant Guidelines, which mandate verification of the legal validity of any demand and the minimization of data disclosure through the careful review and interpretation of all law enforcement demands. The warrant contained mismatched identifiers, as Verizon's records showed that the named individual was not associated with the provided telephone number. Upon detecting the discrepancy, a company employee escalated the warrant for legal review. Verizon's law enforcement legal team contacted the requesting agency, leading to the submission of a modified warrant that dissociated the identifiers. Verizon subsequently fulfilled the request based on the corrected documentation.

This case illustrates Verizon's efforts to ensure government demands are specific and transparent. Furthermore, it demonstrates the effective application of internal procedures to minimize the disclosure of customer data through the careful review of government demands.

CASE STUDY:

Child Rights Impact Assessment Case (Wikimedia)

This case involved the Wikimedia Foundation's first ever child rights impact assessment (CRIA), completed in 2023 to better protect youth participating in its platforms. The CRIA was guided by the Wikimedia Human Rights Policy, which is informed by international instruments such as the UN Convention on the Rights of the Child. The Foundation's work to carry out this form of human rights due diligence led to specific policy and structural improvements. Key actions included finalizing a new Combating Online Child Exploitation Policy, providing recommendations for children to protect themselves, formalizing child rights criteria in grant application reviews, and enhancing the governance and structure of the Human Rights Steering Committee. Furthermore, the CRIA provided critical lessons, leading the Foundation to define and approve a formal four-phase HRDD Framework to guide future risk identification and response. The Foundation also focused on engaging its volunteer communities through town halls and workshops to ensure substantive changes had their buy-in and collaboration. This case illustrates the Foundation's

commitment to responsible decision-making by addressing child rights, mitigating privacy risks, and demonstrates how a community-governed organization can effectively integrate human rights due diligence into its operational model to safeguard its global community of volunteers and users.

CASE STUDY:

Challenging Subpoena/Law Enforcement Request (Zoom)

This case involved a law enforcement legal request to Zoom in 2024, which sought detailed meeting transcripts and information regarding several participants over an extended period. To manage this request, Zoom relied on its governance frameworks, including the Law Enforcement Response Guide, the Government Requests Guide, and an internal whitepaper titled "Defending User Data from Government Overreach." These policies ensure that law enforcement demands align with relevant law and the GNI Principles.

Zoom responded by rejecting the initial subpoena because the request exceeded the permissible scope of subpoena, and informed the requestor that a court order was necessary. Subsequent attempts by the authorities to obtain the data via a court order were also rejected because the requests were not served to the correct legal entity or were not specifically directed at Zoom. As a result, the requesting authority did not renew the request.

This case illustrates Zoom's application of its law enforcement response guidance to ensure that government demands conform to established legal processes and the GNI Principles, requiring requesting authorities to provide precise documentation and follow legal protocols to protect user privacy.

CASE STUDY:

EU DSA Compliance Case (Wikimedia)

This case involved the Wikimedia Foundation's compliance with the EU Digital Services Act (DSA). Governance frameworks guiding this work include the Foundation's Terms of Use, Privacy Policy, Office Action Policy, Wikimedia Human Rights Policy, and the HRDD Framework, alongside specialized guidelines for applicable law determination and requests for user information. The Wikimedia Foundation's approach to compliance with the DSA involved integrating a growing body of globally scoped human rights due diligence into its systemic risk assessment (Article 34) while reinforcing its established processes for handling government requests (Articles 9 and 10). For content removal or data requests from EU Member States, the Foundation ensures compliance with DSA requirements while balancing its commitments to users' freedom of expression

and right to privacy. The Foundation's 2024 DSA systemic risk assessment was grounded in preexisting human rights due diligence initiatives, primarily the 2020 HRIA and the 2024 CRIA, which evaluated human rights risks at the global level. This comprehensive global risk registry was filtered using DSA-specific criteria that identified EU-specific systemic risks such as those emanating from harmful and illegal content. The case illustrates the practical implementation of regional digital rights laws and the integration of human rights due diligence into a community-governed organization.

CASE STUDY:

User Data Request from Azerbaijan (Anonymous)

In 2023, a GNI member company received a request from Azerbaijani law enforcement to disclose user data related to accounts that they alleged were linked to terrorist activity.

In line with the GNI Principles and the company's established policies and practices, following an initial review of the request, the company sought additional context from law enforcement and conducted open source research. After assessing all available information, the company determined that the request was not supported by indicators visible to the company, was overly broad, and was not consistent with international standards. Accordingly, the company declined to produce any data and instead informed Azerbaijani law enforcement that it would need to utilize formal mutual legal assistance channels with the company's home jurisdiction if it wished to pursue the request further.

This case illustrates an example of a GNI member company implementing its policies for responding to law enforcement requests for user data consistent with the GNI Principles, including pushing back on requests that are overly broad or inconsistent with international human rights standards.

CASE STUDY:

Entering a New Jurisdiction (Zoom)

This case involved Zoom entering an agreement in 2023 with a government-owned conglomerate to provide unified communications and collaboration services. To facilitate this, the company engaged in extensive discussions with the foreign government to evaluate relevant regulatory considerations and risk mitigation options. The company utilized several governance frameworks to guide this process, including its Acceptable Use Guidelines, the Government Requests Guide, the Privacy Statement, and the Code of Business Conduct and Ethics.

In response, Zoom's global intelligence team conducted a risk assessment covering government intentions, reputational risks, and physical security. During discussions with the foreign government, Zoom highlighted its commitments to user privacy, security, and freedom of expression, and its policy to challenge overbroad or unlawful requests. Zoom coordinated with the relevant agency of the foreign government regarding data security and ensured the Board and senior leadership were regularly updated. Additionally, Zoom incorporated contractual requirements to comply with GDPR privacy by design and data minimization principles, provided end-to-end encryption where feasible, and certified that no backdoors were created. The company further insisted that any government requests for information follow the protocols established in its Government Requests Guide.

This case illustrates Zoom's due diligence processes when entering new jurisdictions, ensuring that its commercial expansions are consistent with the GNI Principles and Zoom's core values and principles regarding privacy, freedom of expression, and responsible decision-making.

CASE STUDY:

Protecting User Privacy in a Democracy (Wikimedia)

This case involved a request from a lawmaker in a democratic country for internal communications and user data to investigate interactions between the Wikimedia Foundation and various entities. The Foundation's approach was guided by its Terms of Use, Privacy Policy, and Access to Non-public Personal Data Policy. These frameworks define the Foundation's relationship with users, the limits of data collection, and the restricted circumstances under which non-public information may be disclosed. The Foundation responded by evaluating the legal basis of the request and responding narrowly to the request. Furthermore, the Foundation clarified that its privacy policy prevents it from collecting data that identifies a user's citizenship. It also emphasized that, per its Terms of Use, it does not take an editorial role in moderating content on Wikipedia, which differentiates its model from commercial social media platforms. This case illustrates how the Foundation's commitment to data minimization and editorial independence of volunteer contributors helps uphold user privacy and freedom of expression in the face of overreaching government inquiries.

CASE STUDY:

Request Related to AI-Generated Responses (Anonymous)

A GNI member company received an informal request from a state in Asia to correct allegedly outdated and incorrect information about how to report scams to local authorities that was being provided by the company's AI assistant.

As the request was novel—both in its nexus to AI-generated information and informal nature—the company convened a cross-functional team across its policy, legal, product, and human rights functions to review it and respond. The company ultimately determined that the request did not constitute a legal demand; instead, the company treated the request as product feedback related to and deemed it consistent with the GNI Principles and broader human rights commitments to correct the information provided. Accordingly, the company implemented a customized response to similar requests, providing updated and accurate information on how to report scams to local authorities.

This case illustrated how a GNI member company applied the GNI Principles to a novel product and new type of informal government request related to expression.

CASE STUDY:

Israel/Palestine Conflict (Meta)

This case examined Meta's approach to applying the GNI Principles and managing potential human rights impacts—including tensions between freedom of expression and other rights—during the renewed Israel-Palestine conflict that broke out following the 7 October 2023 terrorist attacks against Israel.

The case discussed the role of Meta's Corporate Human Rights Policy (CHRP), Community Standards, Crisis Policy Protocol (CPP), process for responding to government content takedown requests, and other relevant policies, as well as the company's Integrity Product Operations Center model (IPOC), in responding to potential conflict-related human rights risks. It also noted how Meta used findings from its 2022 human rights due diligence on Israel and Palestine to inform its approach, as well as how the company published updates on this due diligence in 2023 and 2024 and communicated with stakeholders on its conflict response, consistent with the GNI Principles related to governance, accountability, and transparency.

Meta's specific efforts to address potential freedom of expression impacts in the context of Israel and Palestine were also considered. These included changes to its Dangerous Organizations and Individuals policy to more narrowly remove "glorification" rather than simple "praise" of designated entities; efforts to carefully monitor the impact of its moderation actions for overenforcement; and to employ proportionate moderation measures, such as allowing certain types of potentially sensitive or offensive content to remain available while making it ineligible to be recommended proactively to users.

The case also examined the impact of the conflict on government requests received from other jurisdictions. As an illustrative example, a request from the German quasi-governmental organization Jugendschutz to restrict access to a Facebook group using the banned slogan "From the river to the sea, Palestine will be free" was reviewed. Meta determined that the slogan did not violate its policies—in line with its prior human rights due diligence and as later explained in an Oversight Board case—but that it was obliged to restrict access to the reported group in Germany on the basis of local law.

CASE STUDY:

Protecting Free Knowledge in Authoritarian and Conflict-Affected Contexts (Wikimedia)

This case involved requests from an authoritarian government for the Wikimedia Foundation to alter or remove content on Wikipedia concerning the matter of a recent military conflict. The Foundation managed these requests through several governance frameworks, including its Terms of Use, which clarify its noneditorial role in content moderation, and the Office Action Policy. It also applied the Applicable Law Determination policy to evaluate whether to comply with foreign legal orders based on risk, legal challengeability, and international human rights standards. The Foundation responded by maintaining the existing content, as it adhered to reliable sources and community standards. Despite the imposition of penalties, the Foundation appealed the court orders to defend the human rights of its contributors and the public's right to access knowledge. The Foundation also uses standard HTTPS encryption to ensure content remains available even when individual pages are targeted for blocking by government authorities. The case demonstrates the Foundation's commitment to upholding freedom of expression when navigating complex international legal demands in authoritarian and conflict-affected contexts.

CASE STUDY:

South Asia Case (Anonymous)

The implementation of restrictive content legislation in a country in South Asia prompted discussions regarding the preservation of freedom of expression and the accessibility of online information.

In response, the company engaged internal and external stakeholders to support a rights-protective approach. The company proposed a voluntary industry code of practice and collaborated with a trade association to encourage a stakeholder consultation process. Additionally, leaders from the company met with government officials to discuss the alignment of legislative frameworks with foreign investment goals. To ensure due process, the company

provides education to law enforcement on the requirements for legal removal requests and maintains a high bar for the removal of political speech.

The case illustrates the application of freedom of expression and privacy principles through industry collaboration, multistakeholder engagement and government advocacy to promote and maintain human rights standards.

CASE STUDY:

Acceptable Use Guidelines Case (Zoom)

Zoom updated its Acceptable Use Guidelines (AUG) in March 2023 to enhance transparency and clarity regarding data ownership and licenses. The update was informed by its Privacy Statement, and its AI Companion Security and Privacy Whitepaper, which align with principles of privacy, governance, accountability, and transparency.

Zoom updated its AUG again on August 10, 2023 to clarify the use of Zoom data for AI training - this revision explicitly stated that customer content, such as audio, video, and chat, is not used to train Zoom or third-party artificial intelligence models. This communication was reinforced by a public blog post from the Chief Product Officer. Internally, Zoom improved its organizational processes to increase the visibility of policy updates across teams and ensured that senior management provides sign-off on such changes.

The case illustrates the importance of transparent and frequent communication, as well as establishing rigorous internal review procedures to ensure that public disclosures accurately reflect Zoom's operational practices.

CASE STUDY:

Exit from a High-Risk Market (Anonymous)

This case involved a telecommunications provider's strategic exit from a high-risk market to align with its long-term corporate strategy. To ensure a responsible transition, the company leveraged its Human Rights Policy and a dedicated implementation playbook, alongside its Enterprise Risk Management (ERM) framework. These governance structures were designed to align the exit process with international human rights principles and mitigate risks associated with freedom of expression and privacy.

The company responded by conducting a Human Rights Impact Assessment (HRIA) to identify and prioritize potential risks to users and personnel. This assessment served as a critical tool for developing mitigation strategies and enhancing staff capacity for stakeholder dialogue. During the acquisition process, the company shared its human rights policies and the HRIA with the acquiring entity, offering a six-month post-sale support period to facilitate the transfer of best practices and ensure continuity in human rights management.

This case illustrates the company's commitment to integrating human rights due diligence into its M&A lifecycle, particularly when operating in complex environments.