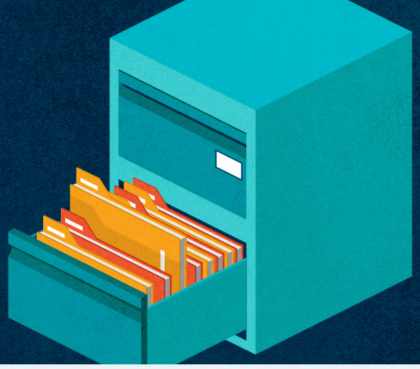
# Selected Company **Case Studies**



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.