Protecting and Advancing
Freedom of Expresssion and
Privacy in Information and
Communications Technologies

Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo

January 2014

1634 I Street, NW, Suite 1100, Washington, DC 20006 ■ www.globalnetworkinitiative.org ■ +1-202-407-8830 ■ info@globalnetworkinitiative.org

Table of Contents

Executive summary

This is the public report on the independent assessments of the Global Network Initiative's (GNI) founding companies: Google, Microsoft and Yahoo. It also includes the first determination by GNI's Board of the three companies' compliance with the GNI Principles on Freedom of Expression and Privacy.

Created in 2008, GNI brings together companies, civil society organizations, investors, and academics to help companies respond to government requests while respecting the freedom of expression and privacy rights of their users. Companies participating in GNI are independently assessed on their implementation of the principles and guidelines. Only assessors accredited by GNI's multi-stakeholder Board are eligible to conduct assessments of member companies. The companies select assessors from among the accredited organizations. Foley Hoag, KPMG, and PwC were selected by the founding companies for the assessments described in this report.

The assessments focus on how companies respond to government requests implicating freedom of expression or privacy rights, looking at a selection of cases arising out of government demands from July 2011 through June 2013. Assessors asked the companies to provide cases based on criteria set out by the assessors, informed by consultation with GNI's non-company participants and independent research. The objective was to select a range of cases that were salient to each company's business model, operating environments, and particular human rights risk profile.

GNI has established a three-phase assessment process. After the completion of the third assessment, the GNI Board makes a determination of compliance or non-compliance with the GNI Principles for each company. A finding of compliance indicates that the GNI Board believes the company has committed to our Principles by adopting policies and procedures to implement them; and based on the cases reviewed, is making a good faith effort to implement and apply them, and improve over time. The assessment process did not and cannot determine whether these policies and procedures are functioning in every case, or whether the company has acted appropriately with respect to each of the many thousands of requests received each year from governments.

Based on its evaluation of each independent assessor's report and other information described herein, GNI's Board determined that Google, Microsoft, and Yahoo are compliant with the GNI Principles. GNI's Board made this determination at GNI's Board meeting in Washington DC on 21 November 2013.

GNI and national security surveillance requests

The news headlines of the last six months have brought to the world's attention the surveillance practices of the United States and other governments. Protecting the free expression and privacy rights of Internet users around the world—the goal behind the creation of GNI—has never been so vital. It was not possible, however, to assess the way in which GNI companies respond to U.S. national security requests because of the restrictions under U.S. law that prohibit the companies from disclosing any information related to such requests. This strengthens our belief that legal and policy reform is necessary and advocacy for increased transparency and other changes will be a greater part of our work in future.

Key findings from the assessments illustrate the challenges that companies are facing across a variety of operating environments.

- The limitations on independent assessments regarding secret national security requests, where companies are prohibited by law from disclosing information about those requests, reinforce our conviction that significant reform by governments is urgently necessary.
- Implementing the principles during acquisitions—and with partners, suppliers, and distributors—remains a challenge. The use of contractual language to limit third party disclosure of company user data can be an important tool in this regard in various ways across the companies. The pace of acquisitions in the technology sector, where many acquisitions are highly confidential and time sensitive, also present a challenge for ensuring that human rights risks are integrated into the due diligence process.
- Decisions on whether content violates a company's Terms of Service when facing government restrictions should be subject to appropriate internal review to ensure the company's compliance with its commitments to the GNI Principles.

This is the first time, to our knowledge, that such assessments involving case reviews of these types of requests have been undertaken by any organization. A number of challenges were encountered, including limitations on assessor access to company information due to assertions of attorney-client privilege and other concerns identified below. Although assessing internal company policies and procedures for responding to law enforcement and other government requests in a highly charged legal environment is a complex undertaking, this report describes the significant progress we have been able to achieve.

In 2014, GNI will carry out a review of the assessment process to integrate learning from this first cycle of assessments, as we also begin assessments of new company members. We expect that the process will evolve over time, and we look forward to working with additional companies as they join us in our work to protect privacy and freedom of expression around the globe.

Introduction

GNI brings together companies, civil society organizations, investors, and academics to forge a common approach to protecting freedom of expression and privacy rights in the Information and Communications Technology (ICT) sector in the face of government requests that may conflict with international human rights standards. Governments have obligations to provide security and protect human rights, and companies have legal responsibilities to comply with legitimate government actions to address national security concerns and uphold the law. But technology companies increasingly face pressure from government requests that could undermine the rights of their users and conflict with the corporate responsibility to respect human rights, as outlined in the United Nations Guiding Principles on Business and Human Rights.[1] The "Protect, Respect and Remedy" Framework, ultimately codified as the UN Guiding Principles, informed the development of the GNI Principles.

GNI seeks to foster multi-stakeholder collaboration to engage with governments and promote and protect privacy and freedom of expression. Given the pressure governments often place on technology companies, the GNI Principles and Implementation Guidelines provide a framework for companies to respond to government requests, backed by a process of independent assessment of company implementation to provide accountability.

In the discussions that led to the launch of GNI in 2008, public attention was on the freedom of expression and privacy risks facing companies operating in repressive and authoritarian countries. Companies operating in such environments should consider potential conflicts between local laws and international human rights standards and how to address such conflicts.

While the challenges in repressive environments remain substantial, the recent disclosures regarding U.S. and other government national security surveillance have shown that significant challenges are present in more democratic regimes as well. At the time GNI was founded the participants understood that companies faced legal restrictions, such as nondisclosure obligations under Foreign Intelligence Surveillance Act (FISA) orders and National Security Letters (NSLs), that prevent them from talking publicly about such national security requests.

However, the revelations in June 2013 about the extent of national security surveillance by the United States and other democratic governments have dramatically brought these issues into the global spotlight, shifted the public debate, and underscored the need for policy reform in many areas. GNI is working together with its members and other groups to call for greater transparency and specific reforms to surveillance practices, not just in the United States but also around the world.

Given that all three companies could not even confirm whether or not they had been subject to national security surveillance demands by the U.S. government under FISA, much less provide any details had they received such a request, carrying out an assessment of the companies' response to such requests was not possible. This reinforces our conviction—what we believe to

[1] UN Guiding Principles on Business and Human Rights available at www.ohchr.org/documents/publications/GuidingPrinciplesBusinessHR_EN.pdf.

be a broad consensus—that reform is necessary. Governments must be more transparent about the requests they make, and should enable companies to be more transparent about how they respond. GNI will continue to work collaboratively with its members to address these concerns. In particular, GNI has urged the 21 governments who have made a formal commitment to respecting online rights by joining the Freedom Online Coalition to take the lead in setting an example in this area.[2] The next meeting of the Coalition in April 2014 in Tallinn, Estonia, will be an important opportunity in this regard.

This public report is the culmination of the first cycle of independent assessment exploring how companies respond to government requests affecting free expression and privacy. This process was conceived and developed as a genuinely multi-stakeholder collaboration, which has also provided an opportunity for experts and organizations with diverse perspectives to work together toward the shared goal of protecting rights online.

The GNI assessment process, although a work in progress, represents a significant step forward. We expect that the process itself, as well as how we report on it, will evolve over time.

The assessment process explained

Companies that participate in GNI agree to a process of independent assessment of their implementation of the principles and guidelines.[3]

The assessment process consists of three phases:

- **Phase I** consists of **self-reporting** by the founding companies, as detailed in GNI's 2010 Annual Report.[4]
- **Phase II** is a **process review** that assesses whether companies are putting into place the necessary policies, systems and procedures to implement GNI's principles. These assessments were conducted for GNI's three founding companies, Google, Microsoft and Yahoo during 2011. Details of that process are available in our 2011 Annual Report.[5]
- **Phase III** is a **case review** that assesses a number of specific cases to understand how the companies are implementing the principles and guidelines in practice. This report focuses on the case review of GNI's three founding companies and covers a two-year period, from July 2011 through June 2013.

[2] "GNI Writes to the 21 Governments in the Freedom Online Coalition," available at http://globalnetworkinitiative.org/news/gni-writes-21-governments-freedom-online-coalition.

[3] Key elements of the assessment process were agreed upon during the negotiations that led to the formation of GNI in 2008, including the Principles, Implementation Guidelines, Governance, Accountability, and Learning Framework, available at http://globalnetworkinitiative.org/corecommitments/index.php, as well as the Governance Charter, available at https://globalnetworkinitiative.org/charter/index.php. The development of the assessment process, including the creation of the templates, was overseen by the GNI Governance and Accountability Board Committee, which met on a bi-weekly basis, and was approved by the GNI Board (See Appendix A).

[4] Available at http://globalnetworkinitiative.org/content/2010-annual-report.

[5] Available at http://globalnetworkinitiative.org/content/2011-annual-report.

The assessed companies: Google, Microsoft, and Yahoo

Google

Annual revenue for most recent FY	$50.2 billion for FY ended Dec 31, 2012
Number of employees and business locations	46,421 full time employees as of September 30, 2013 (including 4,259 from Motorola Mobile). Google has offices in more than 40 countries around the world.

Microsoft

Annual revenue for most recent FY	$77.8 billion for FY ended June 30, 2013
Number of employees and business locations	99,000 employees and subsidiaries in over 100 countries.

Yahoo

Annual revenue for most recent FY	$5 billion for FY ended Dec 31, 2012
Number of employees and business locations	Approximately 11,700 employees, with offices in more than 30 countries, regions, and territories.

Each company identified the scope of business activity subject to review, and focused on products that in the company's view posed the most salient risks to freedom of expression and privacy. Products and services at the three companies covered in cases involving specific requests included search, email, and photo and video sharing services.

Who are the assessors?

Only organizations accredited by GNI's multi-stakeholder Board are eligible to conduct assessments of member companies. Accredited assessors must meet GNI's publicly available independence and competency criteria.[6] Competency requirements include subject matter expertise as well as skills and experience in human rights compliance and assessments or assurance. The independence criteria include factors that would disqualify assessors (e.g. employment or appointment with a GNI company during the past five years), and those that could cause a conflict of interest and must be disclosed. Assessors are subject to re-accreditation on a regular basis (at least every two years).

In November 2012, GNI called for organizations to apply to become accredited assessors. Five applications were received, and following a review by GNI's Board, including additional engagement discussions with the potential assessors, the five applications were approved. It is our plan to increase the number of accredited assessors over time, developing a diverse pool of accredited assessors that reflects and can accommodate the diversity of companies, from small start-ups to major multinationals, in the ICT sector.

[6] Independence and Competency Criteria available at: http://globalnetworkinitiative.org/sites/default/files/GNI%20Independence%20and%20Competency%20Criteria%20for%20Assessors.pdf.

Our current accredited assessors are:

Corporate Context[7] provides consulting, auditing and assurance services in the fields of Corporate Responsibility and Integrity. Corporate Context is managed by Dr. Helena Barton, a social anthropologist specializing in corporate responsibility/sustainability strategies, management systems and communication.

Foley Hoag LLP is a law firm with a Corporate Social Responsibility (CSR) practice that has developed a comprehensive understanding of the human rights challenges facing the ICT sector. They currently advise several leading Internet firms on human rights and legal compliance issues, and are developing a CSR guide for early-stage technology companies in collaboration with the Berkman Center for Internet & Society at Harvard University. Members of their assessment team are also members of the firm's Security and Privacy Practice Group, which is a market leader in developing privacy, safety, and security standards for users and providers of IT services and in helping companies respond to information security incidents.

KPMG AG is the Swiss member firm of KPMG's global network of professional firms providing Audit, Tax and Advisory Services. The global KPMG network consists of more than 155,000 employees working in 155 countries. Data privacy, data protection and corporate social responsibility are key areas where KPMG provides advice and assessments to clients around the world. KPMG's assessment team has acquired in-depth ICT-sector knowledge through the performance of comprehensive operational risk assessments for multinational ICT companies in Europe and worldwide. KPMG AG is accredited for performing certifications according to a number of international standards and has advised and supported governmental agencies in the development of regulations, guidelines and certification programs on data protection and human rights.

PricewaterhouseCoopers LLP is the US member firm of the global PwC network. Each member firm is a separate legal entity. PwC helps organizations and individuals create the value they're looking for. They are a network of firms in 158 countries with more than 180,000 people who are committed to delivering quality in assurance, tax and advisory services. Their US Technology practice is based in San Jose and has particular concentrations in IT privacy, safety, and security standards, database forensics, and operations and product development. Their team has conducted responsible supply chain assessments for companies in the ICT sector based on human rights frameworks including the UN Guiding Principles on Business and Human Rights, as well as engagements focused on privacy.

SSP Blue has extensive experience providing clients with strategic business consulting in the safety, security, and privacy (SSP) arena. Founded in 2010 by Hemanshu Nigam, SSP Blue was retained by GNI to help build the assessment template for the Phase III assessments. A former federal prosecutor in the U.S. Department of Justice, Nigam participated in building the criminal compliance programs at Microsoft and MySpace and currently helps online companies when building such programs at the national and international levels.

[7] In August 2013, Corporate Context was acquired by Deloitte Statsautoriseret Revisionspartnerselskab, a member of Deloitte Touche Tohmatsu Limited.

Assessor orientation

In February 2013, GNI held a daylong orientation for the newly accredited assessors. Civil society organizations, investors, and academics provided the assessors with a detailed briefing on the expertise and resources within GNI that could be drawn on during the assessment process. GNI members also discussed the most salient freedom of expression and privacy risks that the assessment process should address (see text box), as well as key concerns regarding how each of these risks is handled by companies. This orientation is distinct from the specific engagement between the assessors chosen to carry out company assessments and members of GNI's non-company constituencies that is described later.[8]

Issues identified by GNI for consideration in the assessments

Freedom of Expression	Privacy
Blocking/filtering: preventing content from reaching the end user by preemptively blocking entire pages or websites or ad-hoc filtering content based on keywords. • *Using State's own technology*. • *Intermediary liability:* States compelling companies to block/filter ("self-censorship"). **Takedown requests:** a State security body or agency, or an individual, submits a formal or informal request for a company to remove online content. • *Formal:* written, specific as to the target and relevant supporting law, from identified official. • *Informal:* oral or in non-official writing, usually lacking some or all of the above specifics. **Criminalization of speech:** laws make illegal expression that should be legal according to international human rights standards. Legislators claim to be protecting national security, public morals, etc. Security forces shut down, harass, arrest, torture, or execute the "offenders." **Intermediary liability:** companies are held responsible for the content posted by users. **Selective Enforcement:** using legitimate	**Content Surveillance:** broad or targeted surveillance of online activity. • *Broad:* scan all content for specific keywords, email addresses, etc. • *Narrow/Targeted:* surveillance of content received or produced by known activists. **Requests for User Information:** States wish to curtail anonymous expression so they can track, harass, arrest, detain, etc. individuals who express certain views. • *Real name registration:* require companies to require users to use their real name to use the company's website, making it easier to connect activity to an individual. • *Formal requests for user information:* States make formal, written requests for identifying information (real name, location, history of online activity, etc.) that cite to relevant local law and come from a government official. • *Legally unsupported requests for user information:* officials make oral or informal written requests, or fail to identify from which government office the request has come, and do not cite to relevant local or other law. • *Data retention laws:* States require companies to retain certain data for proscribed time periods, and generally pair the requirement with provisions that facilitate government access to the

[8] Both the assessor orientation, as well as the consultations with non-company constituencies on each company's assessment, preceded the NSA revelations of June 2013.

Freedom of Expression	Privacy
enforcement tools to curb political dissent, rather than to achieve law enforcement objectives. Where a law is broadly unenforced, a State may enforce only against some groups as cover for repressing their expression.	retained information, making surveillance easier.

Each company selects a GNI-accredited assessor to conduct its assessment. Foley Hoag, KPMG, and PwC were selected by the founding companies for the assessments described in this report. Although each company contracts directly with and pays its assessor, all accredited assessors also enter into overarching agreements with GNI.

Conducting the assessments

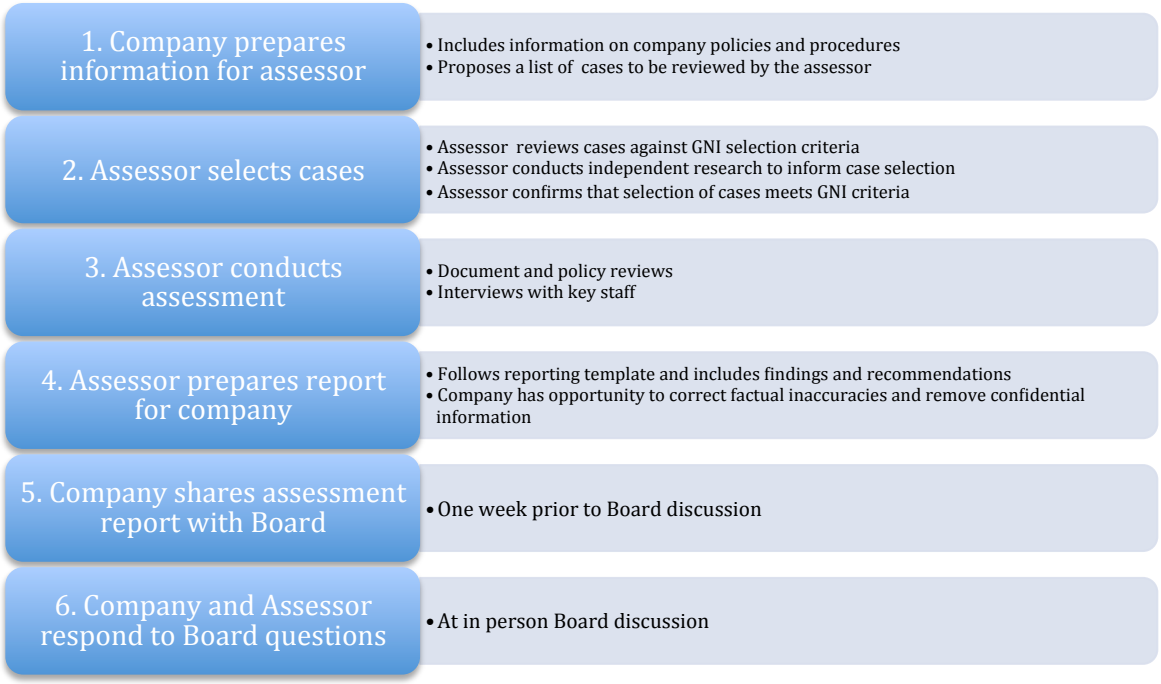
In addition to the independence and competency criteria, three other documents guided the assessment process. See Appendix B for a summary of each of these documents:

1. **Assessment template.** This template gives guidance to the assessors on the assessment process including specific guidance on the case selection process.

2. **Reporting template.** This template sets out the requirements for the assessors reporting to GNI's Board on the outcome of the assessments.

3. **External reporting template.** This framework has guided what GNI would say publicly on the assessments in this report.

The assessment process follows the steps described below:



Case selection

Subject to confidentiality and trade secret concerns, discussed below, assessors sought to determine how companies responded to government requests and demands involving freedom of expression or privacy, in the context of particular cases. This requires a methodology for selecting the specific cases to be reviewed. The assessor was responsible for determining that the cases selected met the GNI criteria, based on requests received by the company, consultation with GNI's non-company participants, and independent research. The objective was to assess a range of cases that were salient to each company's business model, operating environments, and particular human rights risk profile.

The case selection focused on actual cases arising out of government demands during the previous 24 months.[9] What constitutes a "case" was somewhat flexible to cover a range of scenarios. For example, some cases consisted of a single instance or multiple sets of similar requests, or showed how a company operated in a particular environment, rather than how it responded to a specific request.

The assessors consulted with GNI's non-company stakeholders, who identified specific countries where freedom of expression and privacy are at risk and correlated those environments to various forms of restrictions and other concerns. Non-company stakeholders also identified specific cases for consideration by the assessors. The assessors conducted their own research and reviewed external sources, focusing on the countries where a company member is likely to face the greatest challenges. The assessors developed criteria for cases (types and numbers), the companies provided cases based on these criteria, and the company and assessor agreed to specific cases, following GNI guidance that suggested a range of 12-20 cases. Assessors were required to include in their report information about why any case that was specifically recommended by a GNI stakeholder was not selected for the assessment.

Case selection in context

The review of responses to specific government requests is based on a limited number of cases. It is important to note that only the company knows the full data set of government requests from which the cases are drawn. They do not represent a statistically significant random sample of cases and no inferences can be drawn about the population of requests received by the companies in the past 24 months based on this limited sample. The cases were selected to try to address issues of particular concern and challenges highlighted by the GNI Board and participants, and may or may not be representative of total received requests, or how a company generally responds to requests.

Limits on disclosure

GNI's assessments entail a review by third party assessors of company responses to government requests implicating free expression and privacy. However, both external and internal company constraints limit the information available to assessors. This is one of the most challenging issues that we faced during the assessment process. These limits were recognized at the time of GNI's formation.[10]

[9] Certain cases that were specifically identified by non-company participants were included even though they fell outside this 24-month period.

[10] See GNI Governance, Accountability & Learning Framework.

Specific reasons for limits on disclosure include the following:

- Legal prohibitions – There are situations where companies are legally prohibited from disclosing information. For example, in the United States, companies face non-disclosure obligations covering NSLs and FISA orders.
- User privacy – Companies have legal obligations to maintain the privacy of users' personal information as set out in their terms of service. This can affect a company's ability to disclose information about a case, even if that case is well known and has been publicly reported.
- Attorney-client privilege – Companies choose when they assert attorney-client privilege.
- Trade secrets – Companies may choose to withhold competitive information including trade secrets from the assessment process. The assessment reports are reviewed by GNI's Board, which includes representatives from other GNI company members. An antitrust review is completed on the assessment reports prior to their distribution.

Assessors are required to report to GNI's Board on whether their access to information was sufficient to conduct the assessment. All three assessors indicated this was the case but they all also identified limitations on access to information that required alternative approaches to be taken during the assessment process, for example when they were prohibited from directly reviewing policies and procedures, or case-specific documents, in order to preserve attorney-client privilege. These other approaches included interviews with company employees, as well as reviews of incoming government requests and outgoing company responses.

Determining compliance

Based on a review of the assessment reports, discussions with the companies and assessors, and its own collective knowledge, experience and deliberation, the GNI Board voted on company compliance.

GNI's Board determined that Google, Microsoft, and Yahoo are compliant with the GNI Principles. GNI's Board made this determination at their meeting in Washington DC on 21 November 2013.

A finding of compliance indicates that the GNI Board believes the company has committed to our Principles by adopting policies and procedures to implement them; and based on the cases reviewed, is making a good faith effort to implement and apply them, and improve over time.

The assessment process did not and cannot determine whether these policies and procedures are functioning in every case, or whether the company has acted appropriately with respect to each of the many thousands of requests received each year from governments around the world, or with respect to every decision to enter a market, or to develop, alter or acquire a product or service.

The Board views GNI compliance and assessments as an evolving process. The learning from these first assessments will inform changes to the process in the future. For each company, the assessors identified opportunities for improvement, to be reviewed during the following six months.

Should GNI discover information inconsistent with its determination of compliance, GNI reserves the right to take the steps described in the Governance Charter including identifying corrective action steps, or placing a company under special review.

Understanding compliance

The GNI Principles and Implementation Guidelines provide a framework for addressing government requests to companies that implicate the rights of freedom of expression and privacy. Our framework does not require or expect that companies will violate local law, even when that law is inconsistent with international human rights norms. The GNI Principles do require companies to assess risks to privacy and free expression from local law and take measures to mitigate those risks. GNI encourages companies in some circumstances to use legal means to challenge government requests that may violate human rights, and to participate in policy discussions toward the end of bringing local laws into alignment with human rights standards.

In addition to being an assessment of how the company is meeting its GNI commitments, the process seeks to capture and share emerging best practices, and inform GNI's ongoing work.

Google

The GNI Board determined Google to be compliant with the GNI Principles.

The Board found freedom of expression and privacy are taken seriously within Google, as evidenced by cases escalated to senior management, including to Google's co-founder and CEO. Implementation of the Principles is overseen at the senior management level, with event-driven reporting to the Board, as necessary.

The cases show that Google has conducted Human Rights Impact Assessments (HRIAs) to assess potential threats to freedom of expression and privacy, including in relation to acquisitions as well as to launching products in new markets. Google has developed tools for performing HRIAs in a more consistent manner, and is exploring ways to enhance the documentation of the process. Google is also applying new contract terms for suppliers and partners that present privacy risks.

The cases illustrate Google's processes to review government requests relating to freedom of expression and privacy. Google has expanded the use of a central IT platform through which government requests are processed and related internal and external communications are maintained.

Google's legal removals team prepares a global removal report on a bi-annual basis to provide insights and trends on content removal requests. When Google takes down content as a result of a government request, and when Google holds the email address of the user who posted the content, Google often notifies the user via email and points him or her to the page in the Chilling Effects website which hosts a copy of the government request that resulted in the takedown.

Google began issuing a transparency report in 2010, and in the following years has expanded the data and context disclosed in the report.

Microsoft

The GNI Board determined Microsoft to be compliant with the GNI Principles.

The cases illustrate that Microsoft has processes to review government requests relating to freedom of expression and privacy.

GNI members identified Skype, and particularly Skype's joint venture in China, TOM-Skype, as a particular area of focus and concern. Skype was not included as a case study in this assessment. Microsoft explained that although it had specific time-bound plans to address concerns regarding TOM-Skype, those plans were not yet public, and so could not be included in the November 21, 2013 Board Meeting. Those plans have since been reported.[11]

The assessment indicated that Microsoft maintains robust systems to ensure that its Board and senior officers are fully informed about the GNI Principles. Board oversight has shifted, and the Regulatory and Public Policy Committee now has oversight over GNI implementation. Microsoft has also formally charged a Vice President and Deputy General Counsel with responsibility for day-to-day oversight of company implementation of its GNI commitments.

Microsoft has conducted HRIAs before making decisions on whether to embed certain features within platforms in certain high-risk markets.

The systems, policies, and procedures that Microsoft relies upon to implement the GNI Principles are both mature and subject to review. For example, the company has refined its online product development tools to ensure that questions related to freedom of expression and privacy are raised early on in the engineering of new products and features. The company has also revamped the due diligence procedures it uses to assess risks associated with storing certain user data in different geographies.

Microsoft issued its first two global law enforcement requests reports in 2013, important steps in its communication with users regarding requests for user data.

Yahoo

The GNI Board determined Yahoo to be compliant with the GNI Principles.

Yahoo has established a Business & Human Rights Program (BHRP) with two dedicated team members and virtual global team members who are responsible for leading efforts to make responsible decisions on freedom of expression and privacy. The BHRP reports to the Deputy General Counsel/VP of Global Public Policy, who in turn reports to the General Counsel/Board Secretary and provides regular reports and briefings to the Board and executive management.

The cases illustrate a number of examples where the GNI Principles are established and applied in practice, and that Yahoo has made significant progress related to transparency about government requests.

[11] Skype Big Blog, "A new relationship for a better experience in China," available at http://blogs.skype.com/2013/11/25/skype-a-new-relationship-for-a-better-experience-in-china/.

The cases further illustrate that Yahoo has incorporated the GNI Principles in global internal policies and procedures used by the teams responding to law enforcement requests for user data. Additionally Yahoo's Public Policy team engages in dialogue with governments around the world about existing and proposed legislation related to privacy and freedom of expression.

In 2013, Yahoo published its first transparency report, and also published detailed descriptions of its process for handling government requests for user data.

In 2013, Yahoo filed a motion requesting the declassification and release of opinions related to its formerly classified 2008 challenge and subsequent appeal of a FISA directive in the FISA Court and the FISA Court of Review. According to the Presiding Judge of the FISC, the 2008 challenge and appeal was the one instance in which a non-governmental party substantively contested a directive from the government under FISA in the FISC.

Aggregated findings

The GNI Board makes a determination of compliance for each of the companies. Specific findings from the assessment process are presented in aggregate. These findings, and particularly the analysis of trends related to freedom of expression and privacy rights in the ICT sector, will feed into GNI's shared learning and policy engagement activities, and help contribute to our efforts to affect positive change on the ground.

Why aggregated findings and anonymized cases?

GNI presents this information in aggregate form in order to allow public disclosure of important information that might otherwise raise confidentiality concerns or have unintended consequences. GNI is sensitive to how governments might respond to disclosures about company practices. The Principles and Guidelines address highly sensitive situations in which companies face government requests that may be inconsistent with international human rights standards. As a result, the assessments cover cases in which companies use a variety of means to push back on overbroad requests and, in some cases, challenge governments. Making the cases and strategies public could compromise the ability of companies to respond to government requests in a manner that maximizes respect for users' rights consistent with international human rights standards, or to operate in certain countries. Thus, this report focuses on the actions taken by companies in response to actual cases without identifying the actors involved.

Total number of cases reviewed: 59
Cases involving a specific government request: 47
Specific cases concerning privacy: 30
Specific cases concerning freedom of expression: 17
Cases related to the broader context of company operations: 12

Examples of cases related to broader context:

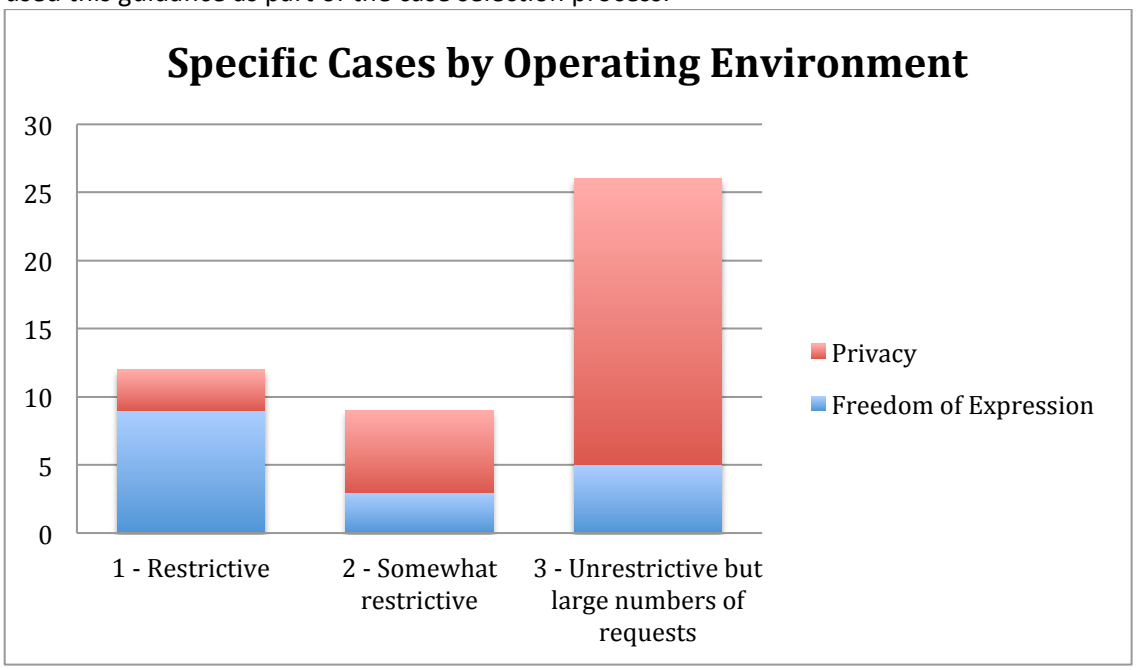
- Transparency reporting
- Selective enforcement of intellectual property laws
- Public policy engagement in specific countries and around the world
- The conduct of HRIAs

Specific Cases by Geography

Asia & Pacific	Australia China India Malaysia Singapore South Korea Thailand
Europe & Eurasia	France Germany Italy Russia Spain Turkey UK
Middle East & North Africa	Jordan Lebanon Saudi Arabia
North America	Canada Mexico USA
South America	Argentina Brazil

Cases by Operating Environment

Guidance provided by GNI's non-company members highlighted threats to free expression and privacy across different operating environments (see Appendix C). The assessors and companies used this guidance as part of the case selection process.



Topics covered by cases

Blocking/Filtering	10
Takedown requests	11
Criminalizing legitimate expression	11
Intermediary Liability	3
Selective Enforcement	2
Request for User Information	29

Some cases covered more than one topic; therefore the total listed here is greater than the 59 cases assessed.

The GNI Principles and Implementation Guidelines guide companies to narrowly interpret government requests and to ensure that applicable legal procedures are followed. Anecdotal data presented by the Phase III Assessments indicates that this approach has resulted in the denial of a number of government requests:

- In 5 freedom of expression cases, requests for clarification or modification contributed to a company deciding not to take action to remove content on a request.
- In 6 freedom of expression cases, the company determined the request stated a clear legal basis and removed the content as indicated.
- In 10 privacy cases, requests for clarification or modification of a request contributed to the denial of a request.
- In 3 privacy cases, a company request to clarify the nature of an emergency contributed to the denial of a request.
- In 13 privacy cases, strict interpretation of jurisdiction and requiring that governments follow established procedures (such as MLATs) contributed to the denial of a request.

Case examples

The following cases have been selected by GNI's Board to illustrate the types of cases included in the assessments. These cases have been anonymized to protect user privacy and preserve confidential information.

Freedom of expression request in Latin America

A company received a request from a judge in a Latin American jurisdiction requesting the removal of user-generated content critical of his rulings. The basis was that the content was in violation of local defamation law. The company responded that the material would not be removed without a court order. The company did not remove the content.

Request to block search results in a restrictive operating environment

A company received a written request from governmental authorities that they block search results inside the country related to a legitimate news story. The company's policy is not to filter or remove access to content protected under international standards of free expression unless it receives a legally binding request from an authorized government representative that such action is required. The company asked the relevant governmental authorities to provide a legal basis for the request. The authorities did not provide a response. The company did not remove the content from its search results.

Content removal in the United States

A company received a letter from a U.S. city attorney addressed to the company's general counsel informing them that a user had posted sensitive content that included photos and plans of a city's public transportation system. The letter explained the publication of this information was prohibited by U.S. federal law and presented a considerable risk to the city's public transportation system from a security perspective, and the content was requested to be immediately removed. The company's law enforcement team worked with a special team in the department that generally handles content moderation or takedown requests and is specifically trained and experienced in handling potentially sensitive issues. The team concluded that the pictures violated the company's terms of service, which prohibit posting of harmful content. The company contacted the user via email, notified him of the request, the city attorney's claim that he had violated the law and that the content violated the company's terms of service, and asked him to remove the pictures from his own account. The user removed the pictures on the same day the letter was received. The law enforcement team informed the city attorney by email the following day that the company had taken appropriate action pursuant to its terms of service. Three weeks later, the Legal team received a follow up email from the city attorney that the removed pictures were still showing up in the search results of another provider, asking the company to direct the provider and other search engines to remove the pictures from their results. The company responded by informing the attorney that they will not request a take down of search results on behalf of third parties, a position supported by the U.S. Communications Decency Act.

Content removal request from outside the United States

A company received a written request from a governmental service in a jurisdiction outside the United States. The request asked that the company remove specific page links from search results. The page links in question led to content that was allegedly unlawful. The company's policy is not to filter or remove access to content protected under international standards of free expression unless it receives a legally binding request from an authorized government representative that such action is required. The company's legal department conducted a legal review of the request, which included consultation with local legal counsel. The company determined that the governmental service did not have legal standing under local law to bring a cause of action against the content in question. The company notified the governmental service that no content would be removed.

Request for user data in Germany

The German office of a company received a letter from a local government agency, attaching a search warrant from a German court requesting the mailbox content of a user subject to criminal proceedings. The court justified in the warrant that it had reason to believe the account holder was using electronic communication in relation to a crime. The court order specified a 6-month timeframe in 2012 when the person was suspected to have committed the crime, but stated that documents from other time ranges, for which no criminal case had been opened, were also subject to this confiscation order as they were required to verify the accusations. The court order further explained the documents released to the authorities which were not related to the criminal case must be immediately deleted by the investigating authorities.

A law enforcement response team member from the German company entity checked that the request was a valid legal process and included all necessary information and approvals, and

processed the request. Based on the assessment that the request was valid, the company produced the emails as requested.

Request for user information in Brazil

The Brazilian legal entity of a company received an official letter from the federal police station of a Brazilian state that was accompanied by a court order issued by a federal judge to wiretap all emails sent and received from a user's email account for 15 days, and to submit those emails to the federal police station. The company's Brazil legal counsel qualified the request as a valid legal process. However, as the stated user account was registered with the company's US legal entity, the request was declined and no data was provided. In the response letter to the federal chief of police and the federal judge, sent two days after the official letter was dated, the company explained that it was technically and legally unable to respond to the request and that Mutual Legal Assistance Treaty (MLAT) procedures would be needed to obtain the requested data from the company's US entity. The letter contained further information about how to contact the US legal entity, informing the requesting agency about the proper legal process to be followed for requesting and potentially obtaining user data.

State law enforcement request in the United States

A State law enforcement official in the United States served a subpoena requesting content and non-content user data from an email account. The company only responds to written requests for customer data that are facially valid and which meet all of the domestic legislative and regulatory requirements of the issuing country. A United States Circuit Court of Appeals decision (Warshak v. United States) held that law enforcement authorities must acquire a search warrant to obtain stored content data from an email account. Based on that legal authority the company requires all law enforcement authorities in the U.S. to obtain a search warrant before it will disclose the contents of communications from an email account. Since a subpoena is not a court order, the company rejected the request from the state law enforcement official.

Company acquisition human rights impact assessment

One case explored the HRIA conducted by a company related to a company acquisition. The company provided limited documentation due to assertions of legal privilege. Interviews with senior representatives of the legal team and limited documentation were used to assess the case. The HRIA identified risks relating to freedom of expression and privacy. It was determined that one jurisdiction presented significant freedom of expression and privacy risks. The company's senior leadership directed the acquisition to be consistent with the company's policy regarding user data in that jurisdiction. A team involving security engineers and individuals from infrastructure, legal, and policy were involved in the HRIA. An implementation plan was developed that included significantly limiting storage of, and access to, user data in the relevant jurisdiction.

For each product and service, the company assessed the risks of having data available locally, made recommendations limiting storage and access to user data for the high-risk jurisdiction, and reported on the implications (e.g. legal, regulatory, technical) of implementation, estimated time and cost of implementing the recommendations, and assigned a person or team responsible for implementation of the recommendations.

Access to user data

One company assessment looked at access to user data as a case exploring the broader context. The company generally applies a "need to know" principle for definition of access rights, only

granting employees access to data they actually need for fulfilling their particular role and job. The company applies global policies related to access to user data that incorporate regional considerations. When a company employee requests new or additional access rights to sensitive user data, a use case will need to be created which follows the defined procedures in an automated workflow tool. The employee will need to open a ticket and justify why access is required for the particular use case. One of the initial questions that need to be answered is if anonymized data can be used for the desired purpose, a mitigating measure to restrict access to sensitive user information. Use cases will be centrally reviewed and signed off by relevant functions (e.g. legal, security, policy). Additional approvers will be triggered for access requests by employees working in sensitive countries or concerning user data from sensitive regions.

The company applies strict procedures and includes contractual language to protect user privacy whenever access to user data is requested by third parties such as suppliers, partners, or contractors. Contractual language restricts or eliminates the ability of third parties contracting with the company to disclose user data. Access rights are generally restricted to the legal entity in which the employee is employed. If a user is registered with a different legal entity, detailed user data cannot be accessed by that respective company employee. However, employees who handle emergency requests for user data or content moderation at the US headquarters have access to user data from all legal entities as they operate a service line for emergency requests on a global level.

Trends and analysis

The findings from the assessments illustrate the challenges that companies face across a variety of operating environments.

Limitations of independent assessments regarding secret national security requests

As noted above, the companies cannot disclose whether or not they have been subject to national security surveillance demands by the U.S. government under FISA. In order to assess how companies respond to such requests, assessors would require access to information that companies are legally prohibited from disclosing. By law, no data related to FISA requests, including the fact that a request has been received or any statistical data on the number of requests received, may be disclosed to users or third parties. Should any information about a FISA request be disclosed, penalties of up to 10 years in prison may be imposed.

Each of the three assessed companies issued public statements and filed legal challenges with the U.S. government in relation to this issue. In addition to the Yahoo challenge described above, Google, Microsoft, and Yahoo have filed suit with the FISA Court seeking the right to share data with the public on the number of FISA requests they receive, and all three companies have publicly supported legislation that would make it possible for companies to report on FISA requests. In December 2013, the three companies joined with other Internet companies to issue principles on Global Government Surveillance Reform, urging changes to practices and laws regulating government surveillance of individuals and access to their information.[12]

[12] See http://reformgovernmentsurveillance.com/.

Implementing the principles during acquisitions—and with partners, suppliers, and distributors—remains a challenge

GNI companies have committed to following the Principles and Implementation Guidelines in all circumstances where they have operational control, and to use best efforts where they do not to ensure that business partners, investments, suppliers, distributors and other relevant parties follow the Principles. The assessments highlight these challenges and make recommendations for how companies can implement their commitments in this area.

Companies with existing contractual relationships that predate GNI commitments may need to work over time to review contracts as they come up for renewal. In these cases, actively focusing on steps to lessen risk in the context of these relationships may be the most appropriate approach in the meantime. One case demonstrated that an HRIA contributed to one company's decision to forego a business opportunity in light of significant human rights risks.

Efforts to address new acquisitions present significant challenges for companies, including how to ensure that human rights risks are incorporated into decision-making at the relevant times given the commercial sensitivity of the opportunities being considered and the pace of acquisitions in the tech sector. Another challenge arises when differences are identified in the compliance systems used for responding to government requests at the newly acquired company. This takes time to address. These challenges are heightened when acquired companies operate in higher risk jurisdictions, or when acquired companies operate in different parts of the ICT sector, such as hardware products, which may face different or novel human rights challenges.

Terms of Service (TOS) enforcement

The GNI Principles state that the right to freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards. Such circumstances include restrictions to preserve national security and public order, protect public health or morals, or safeguard the rights or reputations of others. Decisions about whether content violates a company's TOS should be subject to appropriate internal review to ensure the company's compliance with its commitments to the GNI Principles. This has been an area of focus for shared learning within GNI that could be enriched and informed by the findings from the assessments.[13]

Recommendations

Assessors are tasked with providing non-binding recommendations to the company they assess as well as to the Board. Each company has considered the recommendations from the Phase II assessment carried out in 2011 and in many cases those recommendations have been implemented within the companies. At the Board meeting in November 2013 when the Phase III assessments were discussed the companies committed to report back to the GNI Board within six months on the recommendations they received from their assessor in this most recent assessment.

[13] See http://globalnetworkinitiative.org/gnitags/account-deactivation-and-content-removal.

To the assessed companies

Examples of recommendations made to one or more companies include:

- **Improve the integration of human rights considerations in the due diligence process in relation to acquiring and selling companies.** Ensure that employees working on deals are specifically trained on human rights topics and the GNI Principles, and include key questions in the due diligence process such that, given certain factors or circumstances, human rights teams would be involved in advising on relevant issues when a deal is initiated and before it is completed.

- **Consider the impact of hardware on freedom of expression and privacy,** including the need to update company systems, policies, and procedures to reflect and address specific human rights challenges inherent to hardware products, compared to Internet products and services.

- **Improve external and internal reporting.** This includes, but is not limited to:
    - Consider including government requests for content removal or moderation in future transparency reports, or including more specific reasons for government content removal requests.
    - Provide information on the number of requests received through international legal procedures (e.g. MLATs), and the countries from which such requests originated.
    - Review internal reporting procedures about topics related to freedom of expression and privacy. Consider establishing a semi-annual report to management about human rights topics, which could include data compiled for public reporting and interpretation of that data, along with assessment of regulatory developments (e.g. new legislation), business decisions impacting human rights, and key company initiatives.

- **Review employee access to user data to ensure that employee access rights are restricted by both policy and technical measures on a "need-to-know" basis across global operations.** For example, consider whether employees who only respond to requests related to US registered users need access rights to users registered with international business entities.

- **Review executive management training,** particularly to ensure that new senior executives and board members receive specific training on human rights matters.

- **Improve stakeholder engagement** at all levels to inform decision-making, risk assessments and policy development and implementation.

- **Improve communication with users.**
    - Notifying users of consumer online services when the company provides a government with data (content or non-content) pursuant to a lawful request, unless notification is prohibited by law.
    - Improve public access to company law enforcement guidelines, which should be published for all jurisdictions in which the company responds to compulsory

legal processes. Likewise, facilitate easy access to local terms of service, and to the privacy policies of acquired companies.
    - Improve explanations of what service are or are not offered in particular jurisdictions, the efforts the company makes to promote user safety and privacy and the risks that users face that the company, despite its efforts, is unable to fully mitigate.

- **Increase sharing of best practices.** Consider ways, subject to antitrust, proprietary and confidential information concerns, to share best practices for implementing the GNI Principles and Implementation with peer companies and the GNI membership.

To GNI

A consistent theme across all three assessments was a recommendation to clarify the scope of the assessment and specifically to provide more guidance on how the Phase II process review relates to the Phase III case review assessment. Recommendations to address the scope of the assessments include focusing the assessor orientation and training session on scope and methodology, and consolidating the guidance documents provided to the assessors.

A recommendation to address the challenge of access to information in light of an assertion of legal privilege was to include in the template guidance on minimum level of access to documentation expected for the assessor. For example, this could include contemporaneous and other written documentation of incoming requests and outgoing communications with the requestor. Also provide examples of approaches to work around data access limitations.

Looking ahead

Review process

With the first round of assessments and compliance determinations completed, the GNI Board has the opportunity to reflect on the strengths and weaknesses of the process developed over the last five years, and craft recommendations for strengthening the process. This review will be undertaken during 2014.

Engagement and complaints mechanism

During 2014 GNI will begin implementing a pilot engagement and complaints mechanism based upon a framework developed with the business and human rights consultancy Shift. The pilot mechanism is intended to provide a means for affected parties to raise concerns if they believe that the commitments made under GNI have not been met, consistent with the UN Guiding Principles on Business and Human Rights.

Public policy

Actions by GNI companies, individually and collectively, have shown that even in cases where companies are legally prohibited from acknowledging that they receive national security requests, there are ways for companies to challenge government overreach. Although collective policy engagement has always been envisioned as a key component of GNI, both the revelations regarding communications surveillance and the legal limitations the companies operate under reinforce the importance of policy advocacy as a response. This will be an increased area of focus for GNI in the future.

Appendix A – GNI Board of Directors

Independent Chair
Jermyn Brooks

ICT Companies
Steve Crown, Microsoft*
Ebele Okobi,Yahoo*
Matt Perault, Facebook
Lewis Segall, Google*
Murem Sharpe, Evoca

Note: Three company seats remain open for companies that join GNI in the future.

Civil Society Organizations
Arvind Ganesan, Human Rights Watch*
Leslie Harris, Center for Democracy & Technology*
Robert Mahoney, Committee to Protect Journalists
Tad Stahnke, Human Rights First

Investors
Bennett Freeman, Calvert Group*
Adam Kanzer, Domini Social Investments LLC*

Academics and Academic Organizations
Rebecca MacKinnon, Personal Capacity
Colin Maclay, Berkman Center for Internet & Society at Harvard University*
Deirdre Mulligan, U.C. Berkeley School of Information

Note: Rebecca MacKinnon recused herself from the discussion of the assessments and determination of compliance due to a potential conflict of interest arising from her Ranking Digital Rights Project. Academic Board Alternate Deirdre Mulligan participated in the Board discussion in her place.

* Members of Governance and Accountability Committee

Appendix B – Summary of assessment and reporting templates

Assessment template

The Assessment template was developed from the foundational documents of GNI, the Principles, Implementation Guidelines and our Governance, Accountability and Learning framework.

This template guided both the company and assessor preparation for the Phase III assessment process. It covered the following areas:

Determining compliance
Guidance on how the assessment relates to the Board determination of compliance.

Case Selection
The assessor shall select all cases for review for Phase III. Cases may be provided by the company or by the assessor as part of a consultation process that includes GNI stakeholders.

Any individual cases specifically recommended by a GNI stakeholder or Board member, or significantly highlighted through research of external written sources, should be given particular consideration when deciding which cases to include in the assessment.

Case Review
Assessors must have sufficient access to adequate information within the cases selected and presented for review, keeping in mind the constraints of privilege and the company's contractual obligations to assure the privacy of their users. The template provides minimum suggested characteristics for cases that should be provided to the assessor.

Case Findings
The assessment of cases should be sufficiently robust to allow findings that demonstrate how, and in what ways, a company member is executing against its stated and implemented policies, procedures, and programs to apply the GNI Principles.

Questions for the Assessment

Company description and outline
Relevant to the GNI Principles, information including the scope of business and how it is organized, key suppliers partners and distributors and mergers and acquisitions was requested.

Specific Cases
The template asks what types of government demands the company has received in the previous 24 months and provides a list of factors that cases should illustrate.

Freedom of Expression
- Government Demands, Laws and Regulations – A series of questions in this section of the template sought information on how the company handles government requests including the parts of the company involved in the decision-making process, company actions to minimize the

impact on freedom of expression, engagement with governments and how they work with other organizations when faced with potential inconsistencies between domestic law and international standards

- Communication with users – questions here looked at the steps the company is taking to communicate clearly and transparently with users on its policies and procedures and when access has been removed or blocked because of government restrictions

Privacy

- Data collection – This section focused on the way in which the company evaluates risk associated with the collection, storage and retention of personal data.
- Privacy – Government Demands, Laws and Regulations – Similar to the section relating to freedom of expression, this part of the assessment template sought to understand the policies, processes and procedures the company had in place to protect the rights of users when addressing government demands for data.
- Communication with users – this section asked similar questions to the communication with users section relating to freedom of expression

Responsible Company Decision-Making

- Board oversight and leadership – questions focused on the visibility of freedom of expression and privacy at Board level
- Human rights impact assessments – A series of questions were designed to understand the company approach to carrying out human rights impact assessments including when they were used, how they were updated overtime and how the results of the assessments were used
- Partners, suppliers and distributors – questions in this section were designed to understand how the company determined whether the particular supplier partner or distributor had a material effect on freedom of expression and privacy and what steps the company was taking both where the company does and does not have operational control

Integration into Business Operations

- Structure – a description of the approach the company was taking to implement the Principles was requested
- Integration into business operations – procedures – this section was directed towards the written policies the company had in place, the maintenance of records and means of remediation
- Employees – communication and training of employees were the focus of this section including whether periodic reviews of effectiveness were in place
- Complaints and Assistance – questions in this section focused on whistleblowing procedures and escalation procedures for employees

An opportunity was given for any final comments.

Reporting Template

The Reporting framework gave specific guidance to the assessors in their preparation of the reports at the end of the assessment process, which were distributed to the company and guided the preparation of the redacted report for the GNI Board. This framework covered the following areas:

a. Information about the assessor including relevant experience and expertise
b. Information about the company being assessed
c. The scope of the assessment for example, lines of business, business functions and geographic markets
d. Resources – how the assessment template was applied and feedback on the template. Also an indication if any other resources or standards were used during the assessments
e. Results and conclusions – this was expected to be the largest section of the report covering all aspects of the issues in the assessment template

Appendix C – Summary of non-company guidance to the assessors

Threats to Freedom of Expression and Privacy:
Indicators & Examples across Online Operating Environments[14]

The case selection process should strive to identify a representative set of cases that are salient or illustrative of a company's approach to implementing the GNI framework, given the company's particular products, services, and geographic footprint. What constitutes a "case" can be considered broadly, as defined in the GNI's assessment documentation.

This resource provides GNI participants and assessors with indicators and examples of how government laws or practices require Internet and communications companies to hand over user data, restrict anonymity, or restrict access to content. The categorizations and difficult cases are not intended to be determinative, prescriptive, or exhaustive. Rather, they are intended to inform participants and assessors in their own case selection process by highlighting different operating environments and red flags worth examining.

I. Highly restrictive or repressive operating environments

This category identifies jurisdictions that actively pursue Internet-restrictive policies.

- *Indicators*
  - Key aspects of legal framework impose obligations on intermediaries to monitor users or police online content;
  - Weak and/or oppressive rule of law (e.g., courts not independent in practice);
  - History of selective or abusive enforcement of the law to silence particular users;
  - Restrictions on market entry such as licensing, local partnership requirements, or local data server requirements;
  - Criminalization of many categories of speech;
  - Data retention or real name requirements; and/or
  - User and content surveillance, strong censorship of online media, and requiring companies to hand over user data are commonplace tactics against activists/journalists.

II. Somewhat restrictive operating environments

This category can be viewed broadly. In many of these jurisdictions, the environment for online expression or privacy might be generally free. However, there may be one or two issues that the government deems politically or socially sensitive. For example, the government may be particularly concerned with national security, extremist material/promotion of terrorism, pornography or the protection of children, defamation, insult, or incitement to racial or ethnic hatred.

[14] This Appendix summarizes the guidance provided by the non-company members of GNI for the assessment process in May 2013.

- *Indicators*
  - New regulations imposing intermediary liability introduced during reporting period;
  - Greater enforcement of existing regulations over intermediaries during reporting period;
  - Criminalization of certain categories of speech that may be deemed politically or socially sensitive;
  - Risk of selective or abusive enforcement of the law to silence particular users;
  - Weak rule of law;
  - Restrictions on market entry such as licensing, local partnership requirements, or local data server requirements; and/or
  - Data retention or real name requirements.

III. Generally unrestrictive operating environments with frequent content removal or data requests

These jurisdictions can be identified using available transparency reports released by ICT companies (e.g., Google, Twitter, Microsoft) or through discussion with the company.

- *Indicators*
  - Location of providers' physical operations/employees within operating environment;
  - Greatest number of users located within operating environment;
  - Comparatively strong rule of law and legal processes, allowing much more ability to mount legal challenges against government requests.

IV. Cases raised directly by GNI members or that received heavy press coverage

This category is intended to include cases that have been raised by GNI members or that have received significant media attention over the reporting period. Cases may involve a clear over-reach/human rights violation on the part of the government or action on the part of the company that led to significant human rights harm. If the assessor decides to exclude cases that fit this category from Phase III, the GNI board and external stakeholders will likely seek an explanation of why they were excluded.

V. Other "edge" or difficult cases

This category contemplates cases that present novel or unresolved questions around human rights standards or the responsibility of companies.

This category could also include cases where the company could not achieve a desired outcome, but that demonstrate the company's internal processes and how they dealt with a negative outcome. There may have been a range of internal or external factors for why a company could not achieve a desired outcome, including factors outside the company's control.