

Summary of the GNI's non-company constituencies' guidance for case selection ('case guidance')



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

Threats to Freedom of Expression and Privacy: Indicators & Examples across Online Operating Environments^[1]

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 case guidance provides GNI's 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 indicators and classification of operating environments 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 or where the overall environment for human rights is poor.

- *Examples of 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;
 - Criminalization of many categories of speech;
 - Data retention or real name requirements for internet and telecom companies or cybercafés;
 - Use of network shutdowns during times of unrest; and/or
 - Broad censorship of online and/ or legacy (print, radio, TV) media.

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 or partially free of controls. However, there may be a few 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,

^[1] This Appendix summarizes the guidance provided in August 2015 by the non-company members of GNI for the assessment process in 2015/16.

pornography or the protection of children, defamation, insult, or incitement to racial, religious or ethnic hatred.

○ *Examples of 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;
- Increasing use of website blocking or content takedown requests to social media companies to address politically or socially sensitive categories of speech;
- Passage of new cybercrime, cybersecurity, or counter-terrorism laws that don't adequately protect freedom of expression, privacy, or other rights;
- Risk of selective or abusive enforcement of the law to silence particular users;
- Weak rule of law, with courts susceptible to political influence;
- 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 or through discussion with the company.

○ *Example of Indicators*

- Informal pressure or requests to weaken security or build "back doors" into secured communications;
- 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, as presenting concerns in potential over-reach/human rights violation on the part of the government or action on the part of the company. If the assessor decides to exclude cases that fit this category from the assessment, the GNI board and external stakeholders may 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.