SUMMARY OF CASE SELECTION GUIDANCE
Threats to Freedom of Expression and Privacy:
Indicators & Examples across Online Operating Environments

The case selection process should strive to identify a representative set of cases that are most salient or illustrative of a company's approach to implementing the GNI Principles, 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 Toolkit.

This resource provides GNI participants and assessors with indicators and examples of how government laws or practices require Internet and communications technology (ICT) companies to hand over user data, facilitate abusive surveillance, restrict anonymity, or restrict access to content. The indicators and classification of operating environments are not intended to be determinative, perspective, 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 ICT-restrictive policies or where the overall environment for human rights is poor.

Indicators

- Broad censorship of online and/or legacy (print, radio, TV) media;
- Control over internet infrastructure to limit internet connectivity, permanently or during specific events;
- Centralized telecommunications infrastructure to facilitate control of content and surveillance;
- Legal or de facto monopoly over service providers; high fees and arbitrary requirements (i.e. bureaucratic "red tape," local data server requirements, local partnership requirements) for establishing and operating service providers;
- Filtering and blocking of websites and communication applications (apps) as well as of tools that enable circumvention of online filters and censors;
- Extra-judicial or extra-legal measures used to order the deletion of content from the internet;
- Service providers held legally responsible for the third-party information hosted or transmitted via the technology they supply;
- Key aspects of legal framework impose obligations on intermediaries to monitor users or police online content;
- Very weak and/or non-existent rule of law (e.g., courts not independent in practice) and opaque lawmaking processes that are closed to public participation;
- Weak or unenforced legal protections for human rights, particularly freedom of expression and privacy;

- History of selective or abusive enforcement of the law (e.g., cybercrime or counterterrorism laws) to silence particular groups or individuals;
- Criminalization of many categories of speech;
- Data retention or real name registration requirements for internet and telecom companies and cybercafés;
- Use of offline or online surveillance, including of traditional telecom companies, or requests for user data to silence activists, journalists or political opposition;
- Use of network shutdowns during times of unrest;
- Limits on use of encryption or anonymous expression;
- Mandates to weaken encryption protocols and/or the criminalization of privacy-protective tools.

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

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;
- History of or increased restrictions on legacy media;
- 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;
- Weaker rule of law, with courts susceptible to political influence, though with some ability for civil society and industry actors to participate in lawmaking processes;
- Restrictions on market entry such as relevant licensing, local partnership requirements, or local data server requirements;
- Data retention or real name registration requirements;
- Increased use of digital surveillance and data collection, often without judicial oversight or without meaningful protections for privacy;
- Requests to/pressure on telecommunications vendors to provide monitoring or Lawful Interception (LI) solutions to enable government access to local operators' networks; requests to vendors for direct solutions to block and filter content and websites.

III. Generally unrestrictive operating environments with frequent/high volumes of content removal or data requests

These jurisdictions can be identified using available transparency or corporate social responsibility/ sustainability reports released by ICT companies or through discussion with the company.

Indicators

- Location of providers' physical operations/employees within jurisdiction;
- Informal pressure or requests from the government to "voluntarily" monitor user activity, take down content, or hand over subscriber information, especially to evade legal process;
- Informal pressure or requests to weaken security or build "back doors" into secured communications;
- Comparatively strong rule of law and legal processes, with independent courts and democratically elected legislative bodies, allowing much more ability to mount legal/informal challenges or lobby for reform.

IIII. Other "edge" issues or difficult situations

This category identifies "edge" or "difficult" cases for which there is currently no clear answer or outcome under human rights law. In many instances, these situations present conflicts between domestic and international law; others involve novel or unresolved questions concerning human rights standards and/or the responsibility of companies. We encourage the assessors to include one or more such cases to shed light on and contribute to future learning about how companies are responding in these kinds of situations. Even in difficult situations, there are a range of actions a company may undertake to avoid, respond to, or mitigate potential human rights impacts, including clarifying and limiting government requests and promoting transparency.