

TABLETOP EXERCISE

# Rights-Respecting Responses to Government Demands for Network Disruptions and Emergency Powers



# Table of Contents

|                                                 |          |
|-------------------------------------------------|----------|
| <b>About This Exercise</b>                      | <b>3</b> |
| <hr/>                                           |          |
| <b>Overview of the Current Landscape</b>        | <b>4</b> |
| Industry Landscape                              | 4        |
| Regulatory Landscape                            | 4        |
| Government Demand Landscape                     | 5        |
| <hr/>                                           |          |
| <b>Tabletop Exercise: Hypothetical Scenario</b> | <b>6</b> |
| Country background                              | 6        |
| Industry Background                             | 6        |
| Legal Background                                | 7        |
| Your Role                                       | 8        |
| Government Demands                              | 8        |
| <i>Scenario 1</i>                               | 8        |
| <i>Scenario 2</i>                               | 9        |
| <i>Scenario 3</i>                               | 9        |

# About This Exercise

This fictional tabletop exercise is designed so that relevant stakeholders – including telecommunications companies, civil society experts, and academics working in the areas of connectivity, network disruptions, and user rights — can work together and build on practices to address government restrictions and demands that impact freedom of expression and privacy in rights-respecting ways. The exercise aims to illustrate examples of restrictions and demands governments make of telecommunication providers and last-mile ISPs, the trade-offs these companies need to consider, and how company decisions might impact user rights. This tabletop opens with a contextual overview of the current sectoral and regulatory landscape for telecommunication companies and is followed by the hypothetical “tabletop exercise”.

**This exercise was initially developed as part of a workshop hosted by the Global Network Initiative (GNI) at RightsCon 2023. It is part of a forthcoming series of tabletop exercises produced by GNI that builds off of the [“Across the Stack”](#) tool, which GNI and BSR developed to explore how human rights due diligence considerations, including those around privacy and freedom of expression, intersect with different types of companies across the tech stack.**

# Overview of the Current Landscape

## Industry Landscape

**Telecoms companies and “Last-mile” ISPs** make up a critical layer in the Internet’s infrastructure: they ensure the final connection between backbone ISP’s, which carry the majority of traffic worldwide, and end-users’ networks<sup>1</sup>. Telecom companies build and maintain physical infrastructure while ISPs assign IP addresses and connect devices to the backbone of the internet, handle traffic routing, and manage network capacity. They control the functionality of cell towers and mobile internet, the speed of fixed and mobile connections, and the direction of Internet traffic inside the jurisdictions in which they operate. Telecom companies can play the role of an ISP, especially in mobile networks and ISPs can be built and maintained by Telecom companies.

Most countries allow foreign-owned telecoms and ISPs to operate within their borders. Many countries also operate state-owned telecom operators alongside local and foreign competitors.

## Regulatory Landscape

When operating in a market, companies must ensure that they are compliant with local law. In most countries, Telecommunications regulation is carried out through a framework of regulation and operating licenses necessary to obtain spectrum allocation and remain in legal compliance with the local regulatory authorities

Telecom regulation and operating licenses typically require companies to have in-country offices and staff and provide authorities with several powers that have implications for privacy, freedom of expression, opinion, and access to information. Examples of powers include:

- Law enforcement assistance, such as the provision of real-time lawful interception upon receiving an order,
- Installation of interception equipment that allows direct access by law enforcement,
- Collection, retention, and disclosure of subscriber and communications data.

<sup>1</sup> This classification of companies is from the [“Across the Stack” tool](#).

- Restriction of the network through actions such as through connection slowdowns, website/platform blocking, and total cutoff of mobile or fixed internet connections.
- Limitations on permitted encryption strength.
- National Security and Emergency Powers, such as those to send mass communications dictated by the government to users.

Which entities have these powers, the process of authorization that must be followed by law enforcement when using such powers, the grounds on which these powers can be invoked, and the circumstances that must be met differ from country to country. Such mandates can also include requirements for telecommunication companies to facilitate direct access. For example, GNI's Country Legal Frameworks Resource maps different telecommunication regulations and associated licenses in over 50 countries.

Governments may be invoking the powers outlined in their legal frameworks or making informal demands without legal standing.

## Government Demand Landscape

As noted above, Telecom service providers receive requests including for access to subscriber information, interception, and mandated communications

Consensus that such disruptions constitute a violation of human rights has emerged in recent years alongside a growing reliance on the internet worldwide. Beyond everyday communications, the Internet is increasingly essential for local businesses as well as in the provision of services such as banking or medical services, and disruptions can cause additional direct harm to local people and businesses.

Governments are increasingly ordering network disruptions, especially in response to protests and other conflicts, and during elections. In many cases, companies must weigh their legal and human rights obligations with the risk of license revocation. The GNI principles and Implementation Guidelines ("the GNI Principles") help companies work through these tradeoffs and encourage companies to push back against overly-broad requests. Grounded in the UNGPs and committed to by all GNI member companies, the GNI Principles provide a framework for processes and policies for how decision making around individual demands should be handled in the most rights respecting way possible.

# Tabletop Exercise: Hypothetical Scenario

## Country background

The **Republic of Genovia** is a medium-sized country in the “Majority World”, and will hold presidential elections next year. The incumbent **President** is campaigning for a third term and her party holds a majority in the legislature. The leading opposition candidate is a **Senator**, and a longstanding representative of a minority ethnic group. The Senator has been gaining popularity as a vocal critic of the current administration’s increasingly authoritarian actions.

Three years ago, an unidentified driver tried to crash a van into a crowded square near the Presidential residence; the driver was killed. Independent reports have been unable to verify the attacker’s affiliation, but the President suggested that the driver was affiliated with her challenger, the Senator. Since the attack, public demonstrations in the capital have become more frequent, escalating into violence. The government has taken action against some opposition supporters and journalists, citing threats to public order.

## Industry Background

**TeleWorld** is a multinational telecoms operator based in a rights-protective jurisdiction with strong rule of law, and has sole ownership of Genovia-based **TeleGen**, which is the country’s leading consumer mobile network operator.

TeleGen holds roughly 50% of Genovia’s market share in mobile communications, while domestically-owned **NoviCom** and foreign-owned **Cupid** dominate the most of the remaining 50%. Most people in Genovia rely solely on their mobile devices for connectivity, as they do not have a fixed connection.

TeleWorld is a **Global Network Initiative** member, meaning they have committed to GNI’s Principles on Freedom of Expression and Privacy. In particular, TeleWorld uses the United Nations Guiding Principles on Business and Human Rights to prioritize human rights concerns and impacts.

When salient human rights impacts are identified, TeleWorld considers a range of steps, including conducting rapid and long term human rights impact assessments and then mitigations. TeleWorld has policies on data retention, policies on government access, a procedure for receiving and escalating government requests. Additionally, TeleWorld publishes an annual transparency report.

TeleWorld is closely tracking the situation in the Republic of Genovia and has identified it internally as a ‘crisis’, activating the company’s internal crisis protocols.

## Legal Background

The **Constitution of the Republic of Genovia** guarantees citizens the right to free expression and protects the privacy of citizens and their homes, correspondence, telephone conversations and telegraphic communications. However, the Constitution also permits laws that abrogate these protections if they are “reasonably justifiable in a democratic society in the interest of defense, public safety, public order, public morality or public health.”

The **Communications Regulatory Authority** oversees the telecom sector and administers the relevant regulatory code, which stipulates that The CRA authorizes telecoms licensing. Additionally,

- Licenses are contingent on the installation of any equipment required by the government for monitoring purposes, and authorize the government to take over the licensee’s service in the public interest in the event of a national emergency. Local employees may be held liable for noncompliance with government orders and directions.
- The CRA may order network operators to keep records of traffic data, subscriber information, or related content for 2 years.
- The CRA may order the blocking of mobile terminals in any sensitive area on national security grounds. The licensee must deny service within 6 hours of a legally sufficient request.
- Licenses may be revoked for the “use of the network for anti-national activities,” which is also a criminal offense. No legal document prescribes the method and the instrument that the government may use in this regard.
- The code permits a court or officer in charge of a police station to issue an order for the production of “any document or other thing... necessary or desirable for the purposes of any investigation, inquiry, trial or proceeding.”

## Your Role

You are on a **cross-functional team of senior managers at TeleWorld**. The team includes leaders from the company's centralized Public Policy, Legal (including a Human Rights expert), Policy, and Engineering departments, as well as local representatives from key offices. The team can seek additional expertise as needed from colleagues or other stakeholders.

## Government Demands

You are on a cross-functional team of senior managers at TeleWorld. The team includes leaders from the company's centralized Public Policy, Legal (including a Human Rights expert), Policy, and Engineering departments, as well as local representatives from key offices. The team can seek additional expertise as needed from colleagues or other stakeholders.



### SCENARIO 1

Another public demonstration results in the hospitalization of one of the President's supporters and the arrest of an opposition supporter. In the wake of this, opposition supporters marched again, nonviolently, blocking streets as they moved toward the Presidential residence. The Office of Public Safety contacted the general phone number for TeleWorld and demanded that the company send out an SMS message to all users in city limits. The message should notify users of an immediate curfew and order them to return to their homes or risk arrest.

#### Discussion questions:

1. What are the human rights concerns posed by this demand?
2. What GNI Principles and/or Implementation Guidelines apply?
3. What is the risk of noncompliance?

#### Risk Mitigation questions:

1. What are the next steps available to you?
2. What are the next steps you would take?



## SCENARIO 2

A week has passed since the demonstration. The TeleGen legal team received, via the appropriate form, a request for the identity of every user who was in the vicinity of the Residence after curfew began. Technology to do so is installed and available (per licensing conditions).

### Discussion questions:

1. What are the human rights concerns posed by this demand?
2. What GNI Principles and/or Implementation Guidelines apply?
3. What is the risk of noncompliance?

### Risk Mitigation questions:

1. What are the next steps available to you?
2. What are the next steps you would take? Why?



## SCENARIO 3

In the following weeks, a large demonstration was organized on WorldPlatform, an internationally-based social media platform. Despite warnings from the Genovian government, the demonstration was heavily attended. The President's Chief of Staff appealed personally to the CEO of TeleGen demanding that mobile internet be cut off and forbidding the CEO from public disclosure of the order. The CEO referred the Chief of Staff to the appropriate demand procedure and escalated the matter to you at TeleWorld.

### Discussion questions:

1. What are the human rights concerns posed by this demand?
2. What GNI Principles and/or Implementation Guidelines apply?
3. What is the risk of noncompliance?

### Risk Mitigation questions:

1. What are the next steps available to you?
2. What are the next steps you would take? Why?

