GLOBAL NETWORK INITIATIVE

TABLETOP EXERCISE

Rights-Respecting Responses to Government Requirements for SIM Card Registration

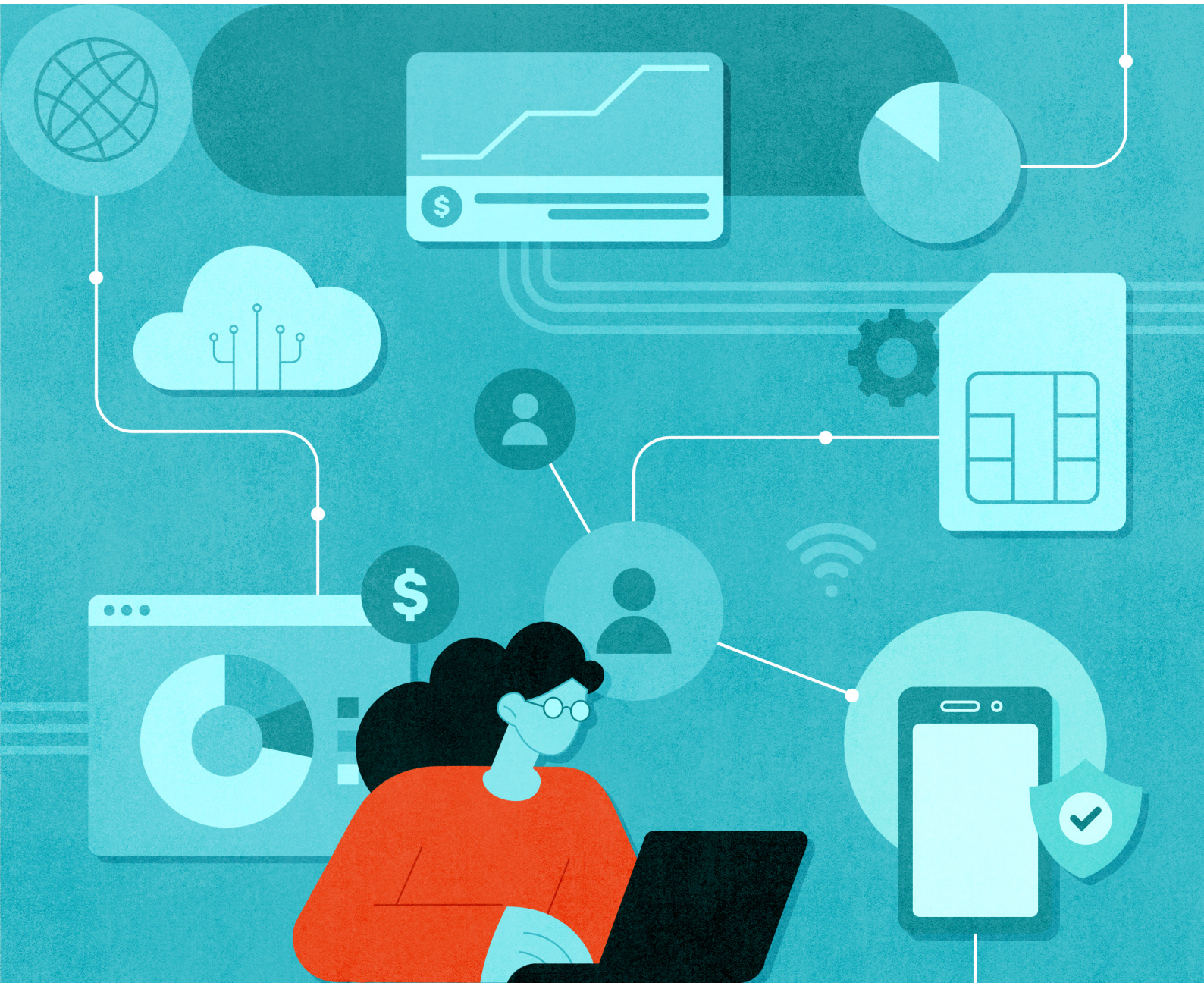

Table of Contents

About This Exercise

This is a fictional exercise designed so relevant stakeholders – including telecommunications ("telco")/mobile service operator ("MNO") companies, civil society experts, and academics who work in areas such as data privacy– can better understand the technical, legal, and policy perspectives of government requirements related to mandatory subscriber identity module ("SIM") card registration. This exercise aims to enhance understanding of the tools, including the GNI Framework, at the disposal of telcos/MNOs to respond to government requests and mandates while upholding human rights.The exercise will explore regulatory developments in African countries as an example of how such requirements are structured and implemented, including an overview of how the local regulatory landscape impacts company decisions, potentially leading to impacts on user rights. This document opens with a technical background around SIM cards, followed by an industry overview and context, and the SIM card regulatory landscape in different countries on the African continent. It then includes a hypothetical "tabletop exercise" where participants simulate being Global Network Initiative (GNI) member telcos/MNOs. As part of the exercise, a designated facilitator provides background information, and walks participants through two government demands. Questions and answers are included for the facilitator.

> **This exercise is part of a series of tabletop exercises produced by GNI that builds on the "Across the Stack" tool, which GNI and BSR developed to explore how human rights due diligence considerations, including those related to privacy and freedom of expression, intersect with different types of companies across the tech stack.**

SIM Cards – A Technical Background

Subscriber Identity Module (SIM) cards are a key component of mobile network communications. They were initially developed in 1991 based on guidelines from the European Telecommunications Standards Institute, with the purpose of connecting a device to a mobile network and storing its phone number. When a user makes a call, sends a text, or accesses the internet, the SIM card verifies that the user is authorized to access the network. For example, if the user has not purchased enough airtime to make a call, the SIM card will connect to the network, determine that the connection is unauthorized, and deny the request.

Each SIM has an international mobile subscriber identity (IMSI) used by the operator to determine the type of plan each user has, which is then charged accordingly. This includes but is not limited to contracted airtime, mobile data, and text messages.

SIM cards have evolved to include more capabilities than just connecting a device to a cellular network. They store text messages, contacts, and other personal information, such as phone numbers. In regions where mobile operators provide mobile money transfer services, identity verification is required through real-name registration. Although financial transactions are not recorded on the SIM card, standard banking sector rules require capturing users' information to prevent fraud, money laundering, and other crimes. Additionally, SIM cards enable account portability, allowing consumers to transfer their telephone number from one device or phone company to another.

Company Overview and Context

Telcos and MNOs ensure the final connection to end-users' networks[1]. These companies may have control over fixed and wireless telecommunications infrastructure, which includes the availability and speed of connections, as well as the ability to control internet traffic. To operate in a given jurisdiction, telcos are granted licenses by the government to acquire and operate wireless spectrum, in accordance with domestic law.

Laws governing telecommunications operation in various countries may address:

- Law enforcement assistance, such as the provision of real-time lawful interception capabilities and oversight of the same
- Collection, retention, and disclosure of subscriber and communications data
- National Security and Emergency Powers
- The ability to restrict access to the network and oversight of the same
- Encryption
- SIM card registration

Companies operating in one jurisdiction while based in another may face consequences for violating the laws of either jurisdiction. Individual companies may collect additional data that they are not legally required to collect, for example, for network optimization and marketing purposes.

[1] This classification of companies is from the "Across the Stack" tool.

SIM Card Regulatory Landscape

According to Privacy International (PI) data from 2020, 155 countries around the world – including 50 African countries – have mandatory SIM card registration laws, with most citing the reasons for their existence as fighting crime, addressing fraud, and protecting national security. SIM card registration is becoming the norm in African countries, as opposed to the exception. A 2021 study of six countries in Africa found that SIM card registration is mandatory in Egypt, Kenya, Nigeria, Senegal, South Africa, and Sudan. The study pointed to a worrying trend where governments are expanding their legal surveillance powers, despite this going against citizens' privacy rights enshrined in African constitutions, international human rights conventions, and domestic laws. Additionally, it found a lack of precision around privacy safeguards in existing surveillance legislation.

When SIM card registration is mandated, operators must ensure they comply with local law, and capture data pertaining to the person who wishes to use mobile services. They usually do so by visually checking a customer's documents, or cross-referencing their identity to a government database. Captured information often includes national ID, physical address, birth date, and sex. Foreigners are often required to provide passport information.

There are three widely known models for capturing SIM card registration information by telcos:

- **Capture and Store:** capture information and store it until it is requested by the government
- **Capture and Share:** capture information and proactively share it with government agency or regulator
- **Capture and Validate:** capture information and validate against a government database

The type of data required for the telcos/MNOs to capture during the process of issuing a SIM card varies by country and domestic laws. For example, Nigeria requires MNOs to register customers using their national identity number, which includes biometrics. Uganda outlines these procedures through the 2023 Regulation of Interception of Communications, companies are required to capture a passport-size photograph, and address for any individual who wishes to obtain service. For Ugandan nationals, companies collect National Identification Cards. Various African governments, such as Ghana, initiated mandatory SIM card registration deadlines that were difficult to enforce, in part, due to people lacking key documents. Even though the Ghanaian

government encouraged people to register their SIM card, provided physical places to do so, and cut-off mobile network access in case of non-compliance, the timeline for customers to register their SIM cards has been rolled back multiple times. The government recently announced it will enforce registration as of July 1, 2025.

Penalties towards telcos/MNOs for non-compliance include heavy sanctions including fines in Gambia up to $595USD, and $1,500 in Rwanda for each SIM card sold without registration. Other measures include cutting off customer access, which violates users rights to access communications and the internet freely. In Tanzania in 2020, 656,091 users were cut off from the network because they failed to register their SIM card.

Some jurisdictions are making moves to store SIM card registrations in a centralized database to make it easier for the government to access and use in fraud and crime investigations. This may include linking SIM card registration with the national ID system. These requirements typically apply to prepaid SIM cards as well as long-term contracts.

Key human rights concerns related to SIM card registration include:

- Mass surveillance; requesting geolocation data
- Exclusion; when an individual's access to the network and associated services is cut off because they failed to register their SIM card due to a lack of documentation, including documentation from informal identity verification sources.
- Inability to communicate anonymously due to communications being linked to the ID of the user.
- Misuse of data and profiling; including matching user data with public and private databases to link someone's data with other data, such as their health records or voting preferences and using the same to inform decisions.
- Cyber Attacks, including gaining access to personally identifiable information, harming someone's right to privacy.

Often, SIM card registration requirements can have further negative implications for the rights of users in jurisdictions with weak data protection frameworks and/or expansive governmental surveillance powers.

Tabletop Exercise: Hypothetical Scenario

Your Role

You work for a large telco/MNO, which is a Global Network Initiative (GNI) member, as a Regulatory Compliance Officer. You have committed to the GNI Principles on Freedom of Expression and Privacy and Implementation Guidelines. Your main duty is to comply with government regulations, to avoid company fines. You collaborate with the Human Rights team at your company, to ensure you are protecting customers against human rights abuses.

Setting the Scene

The Republic of Genovia elects the President, who leads the Executive Branch, every five years through a direct vote. The campaign period for Federal elections lasts six months. Re-election is allowed for one term. Genovia has a multiparty system. Over the past 20 years, the Yellow Party won three elections, but lost the 2020 race to the Aqua Party over their handling of the COVID-19 pandemic. The Aqua party is not doing well in the polls for re-election. There is disappointment in economic growth post-pandemic. People seem to prefer the return to power of the Yellow Party. However, the data available is inconclusive. Some analysts believe the margin between the Yellow and the Aqua party is only 2-3%.

The jurisdiction you are operating in has in place mandatory SIM card registration requirements: you must collect biometrics (face and fingerprints) and the full name from each person who wants to make use of your network through a SIM card. You are also required to capture the identity card information (GenoCard). The law requires you to store this information for one year. You are also required to keep an IMEI database.

The Republic of Genovia grants citizens a constitutional right to privacy and freedom of expression. Currently, there is no data protection law in place. The Interception of Communications Act grants authorities the power to request that telcos provide information about a customer through a court order in cases of national security. Your company offers a mobile money transfer service (G-RAFF).

DEMAND 1

You receive a request for information from the government seeking to identify users 10 meters away from specific polling stations from 6:00 am on the day of election up to two days after the election There is no data protection framework that prohibits you from handing over such user data and your telecommunication license and local regulations require that you hand over data to law enforcement on the grounds of national security.

After making participants know of **Demand 1**, the facilitator will ask the following questions. Mock answers are included in italics to guide the conversation.

1. [Legality] Is the request legally valid? How would you evaluate this?

- *This question covers the principle of legality. Since there is no data protection framework and compliance is a license condition, the loophole that exists allows the government to request this data from you.*

2. [Necessity] Does the government need data it is requesting to meet its objective?

- *The necessity test means the government would need this data to achieve a legitimate aim. If there are less restrictive ways of obtaining the same goal, these should be utilized. You check if the purpose is stated in the order and wonder what the government wants this information for (establishing the aim).*
- *The government has stated the data is necessary given "national security" concerns, and you are required to comply. You question what the link between a polling station, associated with democracy, and national security is. (The government may want to use this data to find political opponents and discourage them from voting.)*
- *You could ask the government to clarify the use, and therefore establish "necessity" for this data.*

3. Do you have the data that is being requested?

- *Technically, telcos know about a user's location through the triangulation of cell-tower information to determine someone's positioning. This means the location of a person is not accurate to the closest 10m (which may be indicative of a polling station). You have the data, but in order to comply, you would have to provide an overbroad swathe of the same.*

4. [Proportionality] Is the request proportionate?

- *According to the proportionality test, the "impact" needs to be proportionate to the legitimate aim. In this case, promoting national security. Companies can refer to GNI Implementation guidance 4.2. This means that, even if the national security concern is real (for example, there may be an armed group), other people's right to privacy information would be impacted. Therefore, the request is not proportionate / over-broad.*

5. Is there an opportunity to push back or narrow the scope of the request?

- *If you chose to push back, and ask the government why they needed the data, and they still gave a vague answer, you can limit the scope of the request to a limited extent given the technology. Ultimately, users outside of the polling space would be impacted.*
- *You would want to note whether the request was made by the government in writing. Given that a distinction cannot be made between the time one user registered over another, you would only be able to provide the information for users who registered a year ago. According to SIM card registration, the information will be deleted after 1 year. This means the company will not have all of the data the government is asking for.*

6. Who in the company should be brought into this decision?

- *According to GNI Implementation Guideline 2.3, companies must have escalation procedures in place to report back to senior management on potential human rights violations.*

7. What short-and long-term mitigations can be taken to minimize the impact on human rights?

- *You ask the government to put the request in writing, engage the authorities about necessity and limiting scope, and refuse to hand over the data. You evaluate what your options are. If you choose not to comply, the government may terminate your license, which may mean you would have to stop providing services and exit the market. You have also had experiences before where the government holds a company employee hostage. You take employee safety very seriously, and do not want to put anyone in harm's way.*

DEMAND 2

The government orders you to provide data located on G-RAFF, the mobile wallet app, where customers store money, pay bills, and receive money. The law requires you to authenticate users by validating their GenoCard information against a government database before allowing them to register for mobile money services. Users can only have access to GenoCard through a SIM card authorized by your network. G-RAFF is regulated as a mobile payment provider. Your company's terms and conditions indicate you are required to monitor account usage and disclose personal information in case law enforcement or governmental agencies with legal powers to do so ask for this information. The government asks you to provide data around specific users (names, transaction amounts, and phone numbers) who may have transferred money to the Yellow party's campaign accounts on G-RAFF citing an anti-money laundering investigation against the Yellow party.

1. **[Legality] Is the request legally valid? How would you evaluate this?**

- *Technically, the regulator is allowed to request monitored transactions in case it suspects fraud or money laundering. While competent authorities are allowed to ask for this information, you are unsure if the authority submitting the request has the specific mandate to do so. You consult with your legal counsel.*

2. **[Necessity] Does the government need the data it is requesting to meet its stated objective?**

- *You seek clarification as to the nature of the money laundering investigation, and how the data supports the investigation. While the Yellow party has shown it is capable of corruption in the past, you fear the Aqua party is asking for this information with political motivation. You also note this is the first time a data request has been received for a purported anti-money laundering investigation. The government does not seem to have provided sufficient evidence to establish "necessity".*

3. Do you have the data that is being requested?

- *Your company has the ability to see the recipient's account (linked to their telephone number) and transactions between accounts. In your terms and conditions, you let users know that you can monitor account usage and disclose information to law enforcement, or any other competent regulatory authority and government agency to assist in the investigation of criminal activities. However, the law does not indicate how long you are required to keep this information. You choose to establish internal data minimization practices where you only keep this data for four years.*

4. [Proportionality] Is the request proportionate?

- *Given the government has not established "necessity", you can narrow the scope of the request. Perhaps there are specific individuals the government has a court order for you to hand over their transaction data. Instead of filtering for every single person who has ever donated to the Yellow party.*
- *In the future, to minimize abuses, you may want to advocate for data protection legislation that would require a company to reduce the amount of personal information they keep or the data retention period, reducing personally identifiable information (PII) storage.*

5. Who in the company should be brought into this decision?

- *Since you are a GNI member company, your legal counsel engaged regulators to push back on the decision citing they have not established "necessity" or "proportionality". The authorities mention they will block the G-RAFFE service nationally if you don't comply, which will cause economic harm to your customers. You comply by providing data related to the top 10 transactions within the last week, and you inform customers their information has been provided to the government as there are no explicit laws or regulations prohibiting you from doing so. In other jurisdictions, you may not be allowed to inform the user given the sensitive nature of a criminal investigation.*

6. What rights are potentially impacted with this request?

- *At a minimum, the right to privacy and free expression. Right to privacy - gives access to the way people use their money. Right to Freedom of Expression - allows the government to identify what user sent a transfer to a political campaign, harming their freedom of speech. Many other rights could also be impacted, e.g. UDHR 21 - right to government / elections.*

GLOBAL
NETWORK
INITIATIVE