Expanding State Surveillance: GNI Raises Alarm on Mexico's new Telecommunications and Security Laws

In July 2025, the Mexican government fast-tracked a series of laws in the Congress which significantly expand the state's surveillance powers and impose far-reaching data retention and disclosure obligations on the private sector. These laws include amendments to the Telecommunications Act, the General Population Act, the Intelligence Act, and the Disappeared Persons Act, and the National Guard and Public Administrations Act. Together, these reforms create an interconnected surveillance infrastructure that mandates biometric identification, establish a centralized repository for a wide range of sensitive data, enable real-time access to public and private databases, compel company compliance without appropriate safeguards, and allow for military surveillance without sufficient oversight. As such, they raise uncomfortable questions about Mexico's commitment to and ability to fulfill its obligations under international human rights law and constitutional guarantees.

The Global Network Initiative (GNI) is deeply concerned by this package of legislative reforms and calls upon the government, as well as the Congress and the judicial sector, to reconsider these approaches by prioritizing the protection of human rights.

Summary of Key Changes

- Telecom companies are mandated to retain user metadata for two years and provide real-time geolocation data to authorities.
- All phone lines must be linked to a biometric ID, or be blocked by May 2026.
- A new mobile user registry requires telecoms to store extensive communication data, echoing the PANAUT system previously struck down by Mexico's Supreme Court.
- All individuals must obtain a biometric CURP ID for public and private services, including iris scans and fingerprints.
- A Unified Identity Platform (PUI) centralizes biometric data and enables real-time law enforcement access.
- The Intelligence Act grants authorities access to all public and private databases, including those of companies across sectors for 'public safety', a word that has not been defined.
- The military and National Guard now have the power to conduct intelligence and surveillance activities without prior judicial warrants.

Regulatory Restructuring Undermining Independence and Oversight

The laws collectively introduce a significant institutional overhaul of Mexico's telecommunications regulatory framework. The reforms replaces the Federal Telecommunications Institute *(Instituto Federal de Telecomunicaciones*, a constitutionally autonomous body known for its technical expertise, pluralistic decision-making, and relative independence from executive control.

In its place, the law establishes two new entities: The Digital Transformation and Telecommunications Agency, a cabinet-level executive agency tasked with formulating digital policy and overseeing infrastructure, and the Telecommunications Regulatory Commission (CRT), a technically autonomous but subordinate body operating under the ATDT.

While the CRT is ostensibly responsible for spectrum allocation, concession granting, and user rights, it is not institutionally independent. The executive branch now controls both policy direction and regulatory enforcement, creating a structural conflict of interest, especially since the Mexican state also acts as a telecommunications service provider in some contexts. In the context of sweeping surveillance powers and burdensome data-retention and provision obligations for private companies, the loss of an independent regulator is especially alarming as it removes a crucial institutional buffer that might have otherwise challenged overreach, mediate disputes, or advocate for due process and user protections.

Sweeping Obligations on Companies without Safeguards

The laws shift surveillance responsibilities onto private companies, including telecommunication providers, banks, healthcare providers, and digital platforms. These companies are required to collect, retain, and hand over sensitive user data, interconnect their databases with government systems and accept biometric CURP and MX Llave credentials for authentication.

These obligations are poorly defined, leaving businesses exposed to legal uncertainty and potential sanctions, including criminal liabilities. These obligations also make it difficult for companies to fulfill ther human rights responsibilities and commitments, creating tension between national law and international business and human rights standards.

Militarization of Surveillance

The law grants military authorities access to civilian data systems for intelligence activities. With the National Guard now under military control and empowered to conduct real-time surveillance without judicial approval, Mexico risks normalizing military-led surveillance in non-military contexts.

In contexts where law enforcement, intelligence gathering, and protest monitoring overlap, this conflation heightens the risk of surveillance being used to suppress dissent or intimidate civil society. Without clear legal limits, transparency requirements, or judicial safeguards, the presence of military actors in digital surveillance ecosystems undermines the rule of law and creates a power imbalance that can be difficult to reverse. These risks are especially acute in a country where journalists, human rights defenders, and Indigenous communities have historically faced targeting and intimidation.

Compulsory Biometric Linkage and a Centralized Surveillance System

The legislative package recreates a provision that closely mirrors the National Register of Mobile Telephone Users (PANAUT), which was declared unconstitutional by the Supreme Court of Mexico in 2022. PANAUT mandated that all mobile phone users link their SIM cards to their biometric data, including facial photographs and fingerprints, and required telecommunications companies to collect and store this information in a centralized government database. The Supreme Court found PANAUT to be a disproportionate measure that violated individuals' rights to privacy, data protection, and access to communication, emphasizing that the law lacked safeguards such as independent oversight, strict purpose limitation, and judicial authorization for data access.

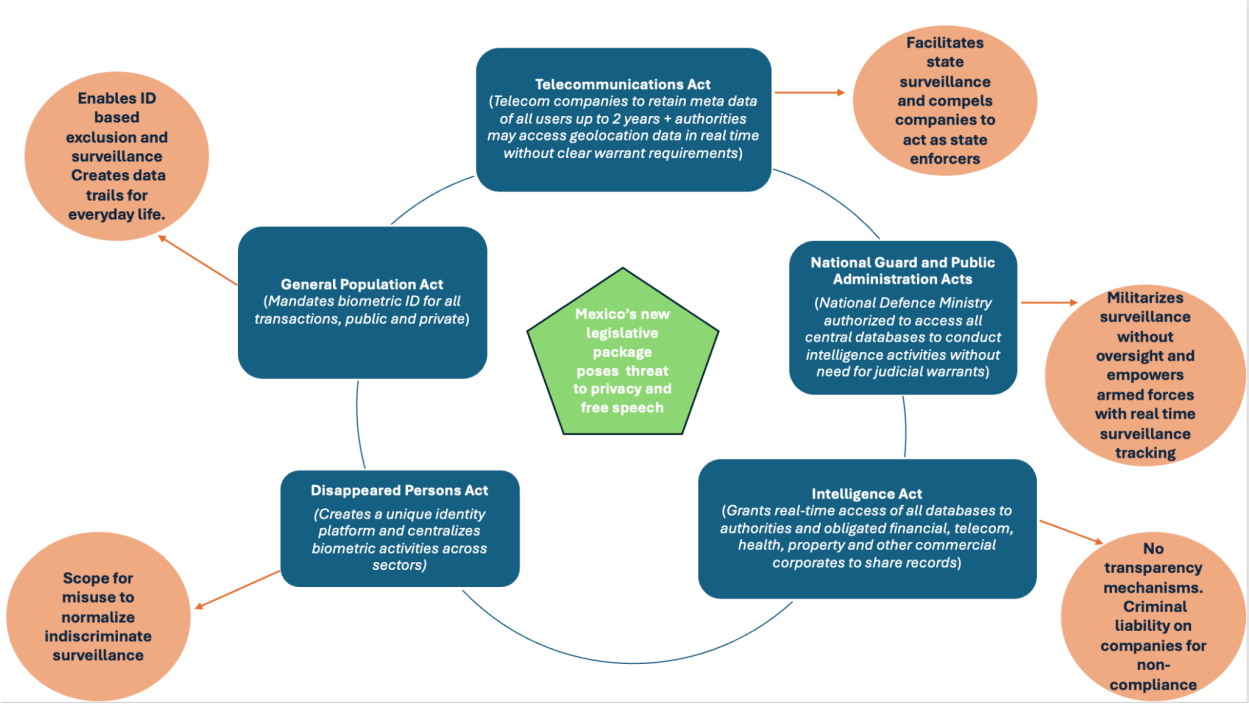
Despite this ruling, the recent legislative package reintroduces a similar registry which must hold all possible telephone lines, along with the obligation to identify every owner with a biometric ID. This structure reproduces the core features that led the Court to strike down PANAUT: compulsory biometric linkage, lack of user control, unclear access mechanisms, and disproportionate interference with privacy and free expression.

In addition, by linking access to basic services with biometric CURP registration and requiring phone service to be tied to biometric ID, the law conditions private activities and civic participation on compliance with systems that can be misused for surveillance. There are

currently no opt-out provisions, meaning that non-compliance is likely to lead to significant economic, social, and political marginalization.

Centralizing vast quantities of sensitive personal information without adequate legal safeguards also creates the potential for data breaches, identity theft, and other illegitimate use, such as where data collected for one purpose is repurposed for unrelated investigations or profiling. In the absence of independent oversight, clear redress mechanisms, and data minimization standards, this infrastructure undermines both trust in public institutions and the principle of proportionality.

What the Laws Do: In Brief



GNI's Call to Action

GNI urges the Government of Mexico to reconsider and revise this legislative package in line with international human rights standards. In particular, we call for:

- Clear and narrow definitions of data access and retention obligations, with appropriate, independent judicial oversight, including the requirement of judicial approval (warrants) for government demands to access user data held by intermediaries.
- Establish strong judicial oversight, requiring independent court orders for any access to user data.
- Provide clarity and legal protections for companies facing government data demands.
- Robust safeguards to protect sensitive personal data, especially biometric identifiers.
- Meaningful transparency and accountability mechanisms for intelligence and law enforcement operations.
- An inclusive, multistakeholder process to assess the human rights impacts of these laws and to ensure that the private sector is not forced to act as an instrument of surveillance without due process.
- Engage civil society, industry, and rights experts in a participatory review of these laws.

GNI is committed to promoting legal and policy frameworks that respect freedom of expression and privacy, and we call on the Mexican authorities to ensure that digital governance advances fundamental rights. We remain available to interact and work together along with the Mexican government to continue engaging on this.

About GNI

GNI brings together more than 100 prominent academics, civil society organizations, information and communications technology (ICT) companies, and investors from around the world. Over the last several years, GNI has reviewed, commented on, and helped shape a range of “online safety” bills across several jurisdictions. Our human rights analysis and recommendations for policymakers can be found in the Content Regulation & Human Rights Policy Brief, which uses international human rights principles to analyze a wide range of legislative efforts and provides proactive guidance on how to address online safety in a rights-protective manner. These recommendations draw on that Brief and readers are referred to it for more detailed analysis.