

FACT SHEET FOR CONGRESS

Venezuela's Digital Repression and Surveillance System

July 7, 2026

*Prepared by Iria Puyosa, Senior Research Fellow
at the Atlantic Council's Democracy + Tech Initiative*

& Andrés Azpúrua, Executive Director at Conexión Segura y Libre.

Submitted for the record of the Tom Lantos Human Rights Commission hearing "Human Rights in Venezuela: Status and Opportunity" (July 15, 2026)

I. BACKGROUND SUMMARY

The sustained use of digital surveillance and control tools by the Venezuelan government undermines prospects for Venezuelan democracy. This [apparatus](#) includes the VEN911 video surveillance system with AI-enhanced facial recognition; mass interception of telecommunications without judicial oversight; the Patria System, which conditions access to welfare on state control of personal data; cyber-patrolling by the SEBIN and DGCIM intelligence agencies; and drone operations used for both intelligence gathering and intimidation. This apparatus impedes the successful advancement of the current [U.S. policy priorities](#) of stabilization, economic recovery, and democratic transition, and runs against Venezuelans' [own aspiration](#) to return to the rule of law and democratic government.

Aside from the formal dissolution of the Strategic Center for Security and Protection of the Homeland ([CESPPA](#)), whose functions were transferred to the Presidential Office, very little has changed in the surveillance system. Self-censorship peaked in January 2026, when [street-level device inspections](#) and cyber-patrolling intensified. The RESORTE-ME Law, the Anti-Hate Law, and the provisions of the Criminal Processing Code grant prosecutors' access to telecom records without a court order. The surveillance apparatus diminishes the chances of holding genuine free and fair elections by [constraining citizens' rights](#) to association, assembly, and expression without fear of reprisal.

Economic revitalization, the second stage of the US framework for Venezuela, presupposes legal safeguards. Lack of data protection, violations of privacy, and constraints on the freedoms of expression, association, and assembly result from the absence of the rule of law. If security forces or prosecutors obtain telecom and financial records without a judicial order, neither a dissident's communications nor property rights can be secure.

Furthermore, the Trump administration has [demanded](#) that the Rodríguez administration wind down the Iranian and Chinese presence in Venezuela, in line with priorities stated in the [National Security Strategy](#). Since critical elements of the Venezuelan surveillance and telecommunications

stack are supplied and maintained by Chinese firms, its continued operation is inconsistent with that hemispheric security goal.

Lastly, the Rodríguez administration's response to the twin earthquakes of June 24 demonstrated their lack of capacity to keep the country stable, secure, and safe. The [state response and the deployment of rescue operations](#) were minimal during the first 48 hours. Still, during that same window, it [activated the collection](#) of additional population data via the government-owned messaging VenApp and the Patria System.

II. KEY DATA

- **VEN 911 integrates thousands of CCTV cameras.** For example, Chacao (the Caracas municipality where visiting US officials and investors typically stay) has deployed more than [300 AI-enabled cameras](#) across five square miles, which can be accessed by national security forces without judicial authorization.
- **Sanctioned Chinese vendors maintain the system.** CEIEC ([sanctioned](#) by the US Treasury in 2020) continues to operate in Venezuela despite sanctions; Hikvision and Dahua (which are on the [Commerce Entity List](#)) supply hardware nationwide; ZTE built the Patria System data platform and the Smart City data layer that underpin VEN911. Likewise, [Huawei expanded](#) Venezuela's national telecommunications backbone.
- **The [Patria System](#) holds ~20 million registered users, roughly 90% of the country's adult population.** Welfare access is contingent on registration. Moreover, the listing of household members and the mapping of community networks enable data collection on unregistered individuals.
- **Private communications interception at an industrial scale.** [Telefónica's 2021 transparency report](#), the last before disclosures ceased, recorded interception of about 20% of Movistar Venezuela subscribers, and metadata (including geolocation) from about 13% of subscribers was routinely delivered to security agencies. Although public transparency reporting is unavailable from national providers, these companies are likely providing similar data to maintain authorization to operate in the country. The state-owned CANTV grants security agencies direct access to communications data without judicial oversight.
- **The linkage between surveillance and arbitrary detentions persists.** Communications interception, cyber-patrolling, and grassroots snitching via messaging apps were integrated into [Operation Knock Knock](#), which led to 1,600 arrests after the stolen 2024 presidential election. Every component of this chain is still functional and can be weaponized by the current authorities.
- **The connectivity network lacked resilience.** The June 24 earthquakes damaged the coastal fiber backbone and knocked out base stations, leaving affected regions without mobile or Internet coverage, hampering rescue coordination and access to emergency

information. The sector regulatory agency, [CONATEL](#), authorized traffic rerouting through neighboring Colombia, the temporary use of LEO satellites for Internet connectivity, and direct-to-device satellite messaging by mobile providers Movistar and Digitel only after hours of disconnection. Civil society organizations Conexión Segura and Redes Ayuda responded by installing Starlink connectivity points for rescue teams and communities.

- **Censorship persisted through the emergency.** More than 200 domains remain [blocked](#), including over 60 news sites, and the messaging app Signal, while the block on social media platform X was partially lifted after the June 24 earthquakes. In June alone, Espacio Público documented [26 violations of information freedom](#), mostly censorship and intimidation, including threats against journalists covering rescue efforts.

III. REQUEST FOR CONGRESSIONAL ACTION

- **Sanctions relief conditioned on verifiable milestones.** Sanctions relief and economic assistance should be conditioned on the verified dismantling of the surveillance apparatus. The research reported in [Watch the Watchers](#)¹ identifies the systems that must be deactivated and the legislation to repeal. That information can help to set dismantling benchmarks that are verifiable through technical analysis.
- **Require periodic State Department reporting on indicators of the dismantlement of surveillance and censorship.** Such reporting will assess whether meaningful change is occurring. This requirement also aligns with the National Security Strategy's objective of reducing reliance on Chinese-maintained critical infrastructure in the Western Hemisphere.
- **Oversight of sanctions enforcement against surveillance technology vendors.** Request that the Treasury and Commerce Departments investigate and report on CEIEC's continued operations in Venezuela despite the 2020 sanctions and impose supply-chain transparency requirements.
- **Appropriate funding for democracy programs in Venezuela, as proposed in the Foreign Aid Bill for FY2027.** In the execution of the funds, ensure that foreign assistance priorities include digital security and connectivity support for Venezuelan civil society, especially secure communications tools, emergency connectivity and response networks, and digital security training.

¹ Azpurua, A. & I. Puyosa (March, 2026). *Watch the Watchers: Surveillance Technologies for Political Control in Venezuela*. Atlantic Council. <https://dfrlab.org/2026/03/26/watch-the-watchers-report/>



John F.W. Rogers
CHAIRMAN

Frederick Kempe
PRESIDENT & CEO

Adrienne Arsht
EXECUTIVE VICE CHAIR

Stephen J. Hadley
EXECUTIVE VICE CHAIR

This memorandum is endorsed by
The Washington Office on Latin America (WOLA)
Acceso Libre
Espacio Público