

Pakistan has emerged as one of the world's most closely watched societies, not by choice, but through the construction of an elaborate mass surveillance architecture that scrutinizes the digital and mobile activities of millions. This vast system—powered by a blend of local enforcement and international technology—has drawn repeated warnings from rights groups and growing condemnation from global leaders, who argue it not only shreds privacy but fundamentally undermines democracy and moral norms.

Anatomy of The Surveillance State

At the core of Pakistan's surveillance system are two powerful tools: the Lawful Intercept Management System (LIMS) and the Web Monitoring System 2.0 (WMS 2.0). LIMS, a tool provided by German firm Utimaco through UAE-based Datafusion, is mandated for use by all major telecom providers under the direction of the Pakistan Telecommunications Authority (PTA). This tool enables security agencies—most notably the armed forces and Inter-Services Intelligence (ISI)—to tap, monitor, and sometimes store nearly all phone calls, text messages, and browsing histories of countless citizens. WMS 2.0, based on Chinese "Great Firewall" technology and upgraded in 2023 using hardware and software from China's Geedge Networks, US-based Niagara Networks, and France's Thales, allows for deep-packet inspection of internet traffic, blocking or throttling up to 2 million simultaneous web connections, with powerful censorship capabilities.

Foreign Facilitation and A Profitable Economy of Oppression

Amnesty International's recent year-long investigation revealed how this entire ecosystem was built with the active participation of companies based in China, Germany, France, the United States, Canada, and the UAE. At least four major mobile operators were ordered to

integrate directly with LIMS, meaning that up to 4 million phone lines can be put under direct real-time surveillance at any moment. Service contracts and equipment deals with telecoms have allowed a seamless, largely unaccountable flow of personal data from the public to both local and foreign entities. "Pakistan's mass surveillance and censorship have been made possible through the collusion of a large number of corporate actors... This is nothing short of a vast and profitable economy of oppression, enabled by companies and States failing to uphold their obligations under international law," said Agnès Callamard, Secretary General at Amnesty International.

For those living under the shadow of surveillance, the effects are both immediate and terrifying. In interviews for Amnesty's report, one Pakistani journalist described living with "the certainty that everything is monitored, be it email or calls," and recounted having to curtail contact with family after a probe into his investigative reporting: "After the story, anyone I would speak to, even on WhatsApp, would come under scrutiny. The authorities would go to people and ask them, why did he call you?... now I go months without speaking to my family for fear they will be targeted". This chilling effect—where the fear of being watched leads activists, politicians, journalists, and even ordinary people to silence themselves—is widespread, shrinking civic space and undermining basic freedoms. In restive regions like Balochistan, whole districts have suffered internet blackouts lasting months or longer, alongside enforced disappearances and targeted harassment of those advocating for basic rights.

Amnesty International, Human Rights Watch, and local digital rights organizations have been unambiguous—these surveillance practices violate not only Pakistan's constitution (which guarantees the right to privacy under Article 14) but also various international human rights agreements. In the words of Jurre van Bergen, Technologist at Amnesty: "Due to the lack of technical and legal safeguards... LIMS is in practice a tool of unlawful and indiscriminate surveillance that allows the government to spy on more than four million people at any given time". Human Rights Watch has characterized the government's approach as prioritizing

“muzzling dissenting voices over protecting the rights of everyone in Pakistan”. Reports document that warrant requirements—supposedly enshrined in law—are routinely ignored or bypassed, as enforcement agencies acquire ever more advanced snooping capabilities.

Inadequate Oversight, Opaque Contracts, Zero Consent

Critical to the outrage is the complete lack of transparency and public consent: not only are citizens almost entirely unaware of the extent of monitoring, but foreign suppliers are rarely forthcoming about the scope of their contracts or the use of their technologies. Out of 20 companies contacted by Amnesty, only two provided substantive answers about their roles or safeguards. The Pakistani government itself provided no response at all. Even Western governments and regulatory authorities—briefed in detail—have responded with little more than perfunctory acknowledgements and have imposed no meaningful controls on the export of mass surveillance technology for repressive use.

Authorities and army officials defend the expansion as vital for “national security,” but the main targets are often nowhere near terrorists or criminals. Instead, journalists, dissidents, human rights defenders, lawyers, and minority community leaders are those most at risk. According to Amnesty, over 650,000 web links—including news sites, social platforms like YouTube, Facebook, and X—are currently restricted, with VPNs and encrypted channels also being blocked “as unlawful”. In court cases such as the leak of private calls involving opposition leader Imran Khan’s family, telecom officials have admitted on public record that mass phone-tapping was requested by the state. The chilling message: “Instead of fighting terrorism,” notes one report, “the real targets are critics of the military establishment, activists, and journalists”.

While Western corporate players are implicated in building Pakistan's surveillance state, several political leaders and watchdogs abroad have criticized the drift toward digital authoritarianism. "Surveillance without oversight is not security but tyranny," notes a report cited widely in Western media commentary on the issue. With China as both a blueprint and technology provider, Western diplomats and UN-appointed digital rights experts have raised alarms that "If fragile democracies like Pakistan embrace Chinese-style digital authoritarianism, it signals to other countries that repression can be imported and democracy can be bypassed". However, as of 2025, few concrete sanctions or trade restrictions have materialized, and many Western firms remain deeply embedded in these networks.

Pakistan's legal framework has failed to keep pace. Domestic laws either lack genuine oversight mechanisms or are actively circumvented; the courts, when approached, have sometimes found the surveillance unconstitutional but are unable to enforce protections. "Unchecked digital repression," warned Amnesty, "will limit space for democracy". Such government overreach not only endangers freedom of expression, assembly, and opinion—it places basic human dignity at risk and threatens to normalize mass surveillance as a tool of governance far beyond Pakistan's borders.

A Moral Imperative for Global Action

Pakistan's drift into surveillance-driven authoritarianism is not a siloed domestic issue; it is a cautionary tale for democracies everywhere. With no meaningful consent, oversight, or regulation, millions live everyday lives under the gaze of the state, backed by a profitable and largely unaccountable global industry. The calls by Amnesty, Human Rights Watch, and other defenders of rights and democracy are urgent and unambiguous: global technology companies, foreign states, and Pakistani authorities must be held accountable for violations, and the mass violation of privacy must stop—before the darkness spreads further.

References and Further Reading

Amnesty International. (2025, September 8). *Pakistan: Mass surveillance and censorship machine is fueled by Chinese, European, Emirati, and North American companies* [News release]. <https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/>

Human Rights Watch. (2024, January 10). *Widening crackdown on dissent in Pakistan*. <https://www.hrw.org/news/2024/01/11/pakistan-widening-crackdown-dissent>

Human Rights Watch. (2024, December 11). *World Report 2025: Pakistan*. <https://www.hrw.org/world-report/2025/country-chapters/pakistan>

Reuters. (2025, September 9). *Amnesty says Pakistan spying on millions through phone-tapping firewall*. <https://www.reuters.com/world/asia-pacific/amnesty-says-pakistan-spying-millions-thorough-phone-tapping-firewall-2025-09-09/>

Al Jazeera. (2025, May 7). *How world leaders are reacting to India-Pakistan military strikes*. <https://www.aljazeera.com/news/2025/5/7/how-world-leaders-are-reacting-to-india-pakistan-military-strikes>

Human Rights Watch. (2025, June 8). *"A conspiracy to grab the land": Exploiting Pakistan's blasphemy laws for blackmail and profit*. <https://www.hrw.org/report/2025/06/09/conspiracy-grab-land/exploiting-pakistans-blasphemy-laws-blackmail-and-profit>

Pakistan's Digital Prison: Mass Surveillance, Censorship, and the Cost
to Democracy

YouTube. (2025, September 9). *Amnesty report exposes Pakistan's mass surveillance and censorship*. [Video]. https://www.youtube.com/watch?v=HA_4BX0pbMs