



SHADOWS OF CONTROL

CENSORSHIP AND MASS SURVEILLANCE IN PAKISTAN

EXECUTIVE SUMMARY

AMNESTY
INTERNATIONAL



Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.



© Amnesty International 2025

Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

For more information please visit the permissions page on our website:

www.amnesty.org

Where material is attributed to a copyright owner other than Amnesty International this material is not subject to the Creative Commons licence.

First published in 2025

by Amnesty International Ltd

Peter Benenson House, 1 Easton Street

London WC1X 0DW, UK

Cover illustration: A series of rooms containing individuals using their digital devices being surveilled by unknown black ghosts with red eyes hovering over the individuals to see what they're doing on their digital devices. In the upper central part of the image there's a giant eye that's hanging on top of a world map. The eye's veins are connected to a world map able to monitor the internet traffic that's connecting to various countries around the world. © Bushra Saleem

Index: ASA 33/0207/2025

Original language: English

amnesty.org

AMNESTY
INTERNATIONAL 

EXECUTIVE SUMMARY

Pakistan has a long and well-documented record of engaging in unlawful surveillance and online censorship that poses grave risks to the human rights of human rights defenders, marginalised communities and, indeed, everyone in the country. These practices continue against a background of an increasingly oppressive political landscape, including the use of draconian laws to criminalize online free expression, a clampdown on protest and assemblies, arbitrary arrests and detentions and enforced disappearances. Pakistan's legal system fails to protect against mass surveillance practices, both because domestic legislation lacks critical safeguards and because the law is frequently ignored or circumvented in practice. This report documents how, rather than reform its practices in line with human rights standards, the Pakistani authorities have obtained new, more advanced forms of surveillance and censorship technologies from a global array of companies.

While Pakistan bears the primary responsibility for the human rights violations resulting from these practices, and has a binding legal obligation to prevent such harm, the authorities have for years relied on technology purchased from private companies in other countries to carry them out. As in many countries – and contrary to international human rights standards – such purchases are mostly non-transparent, allowing exporting companies to evade their human rights responsibilities, and leaving people in Pakistan in the dark about the ways in which they may be surveilled or censored online. With these systems in place, no one is free from the repressive surveillance and control by the Pakistani authorities.

This report sheds light on the private companies around the world who, despite Pakistan's troubling record of protecting rights online, have provided – and in some cases continue to provide – the technology that powers the unlawful surveillance and censorship. It highlights both how these companies have flouted their human rights responsibilities, but also how foreign states have failed in their obligation to adequately regulate the transfer of such technologies to countries where their use would pose clear human rights risks. The report provides specific technical details on the forms of surveillance and censorship technologies that are being sold to the Pakistani authorities and telecommunications providers. This technical information on the products is included to document the evolution of these technologies and the increased capacities they provide to States, in this case Pakistan, to surveil a significant amount of the population without independent oversight and control their access to the internet or certain websites. The technologies featured in the report are at the cutting edge of surveillance and censorship technology, allowing for access to huge amounts of personal data on large portions of the population simultaneously in a form of mass surveillance, as well as deep-packet inspection technologies which facilitate the blocking of VPNs or any kind of traffic deemed unwanted by the authorities. The aim of this report is to provide a comprehensible overview of both the surveillance and censorship mechanisms active in Pakistan, which have been shrouded in secrecy. This secrecy creates an information asymmetry and reduces the ability of civil society to protect itself from mass surveillance or censorship.

The report is the result of the *Great Firewall Export*, a year-long investigation by Amnesty International, in collaboration with IntersecLab,¹ Paper Trail Media and partners, Der Standard and Follow The Money,² The Globe and Mail,³ Justice for Myanmar⁴ and the Tor Project.⁵ The report exposes the extensive trade of digital mass surveillance technologies to Pakistan by German and Emirati companies since 2014, and internet

¹ InterSecLab, <https://interseclab.org/en/home-en/> (accessed on 18 August 2025).

² Paper Trail Media, <https://www.papertrailmedia.de/> (accessed on 18 August 2025), DER STANDARD, <https://www.derstandard.at/> (accessed on 18 August 2025), Follow The Money, <https://www.ftm.eu/> (accessed on 18 August 2025).

³ The Globe and Mail, <https://www.theglobeandmail.com/> (accessed on 18 August 2025).

⁴ Justice for Myanmar, <https://www.justiceformyanmar.org/> (accessed on 18 August 2025).

⁵ The Tor Project, <https://www.torproject.org/> (accessed on 18 August 2025).

ensorship technologies by Canadian companies since 2016 and US companies since 2021. In 2023, Chinese, US and French companies provided technology for Pakistan's upgraded national firewall.

The two most notable abuses that these technologies enable are mass surveillance and unlawful internet censorship. Mass surveillance involves widespread monitoring, collection, storage and/or analysis of sensitive personal data, such as phone calls, text messages and Internet activity, without individualized reasonable suspicion of criminal wrongdoing. In Pakistan, the Armed Forces and the Inter-Services Intelligence (ISI) use the Lawful Intercept Management System (LIMS) to surveil a significant portion of the population's digital activity through Pakistani telecommunications providers (who are required to cooperate with LIMS in order to operate in the country). This has been done without any court warrant by Pakistani security agencies, as revealed in a court case in 2024. Through commercial trade databases on subscription-based platforms, Amnesty International found that a German company, Utimaco, and an Emirati company, Datafusion, supplied most of the technology that enables LIMS to operate in Pakistan. Utimaco's LIMS allows the authorities to sift through the telecommunications provider subscriber data which is then made accessible through Datafusion' Monitoring Center Next Generation (McNG). Due to the lack of technical and legal safeguards in the deployment and use of mass surveillance technologies in Pakistan, LIMS is in practice a tool of unlawful and indiscriminate surveillance that allows the government to spy on more than 4 million people at any given time.

Internet censorship involves blocking specific content on the internet, slowing down and controlling internet speeds, or shutting down the internet altogether. In Pakistan, online content such as websites and social media platforms like Wikipedia, TikTok and X are routinely blocked, and internet and network shutdowns are frequent. Nationwide shutdowns were documented during the 9 May 2023 protests and the February 2024 elections, as well as localized and province-wide shutdowns on other occasions. To identify and block online content, the Pakistan Telecommunications Authority (PTA) uses the Web Monitoring System (WMS) through local telecommunications providers.

Based on existing research and commercial trade databases on subscription-based platforms, Amnesty International found that a first iteration of the WMS was installed in Pakistan in 2018 using technology provided by a Canadian company, Sandvine. Amnesty International has found Sandvine to appear in trade-data as early as 2017 and having shipped equipment to at least three Pakistani companies who all have a history of working for the Pakistani government, two of which have not been named before: SN Skies Pvt Ltd and A Hamson Inc. Through a leak that was shared with the consortium, and which is referred to by Amnesty International as the Geedge dataset, Amnesty International also uncovered that the previous WMS, which Amnesty International refers to as WMS 1.0, was later replaced and advanced using new technology produced by a Chinese company, Geedge Networks. Hardware components were shipped to Pakistani company ELC Solutions Pvt Ltd. by a Chinese state-owned subsidiary of China Electronics Corporation via its subsidiary, ELINC China Co Ltd. Amnesty International believes that the technology provided by Geedge Networks is a commercialised version of China's "Great Firewall", a comprehensive state censorship tool developed and deployed in China and now outside as well. Installation and operationalisation of the WMS provided by Geedge Networks in Pakistan was enabled by software or hardware from different companies, including US-based hardware from company Niagara Networks, licensing software from French company Thales, and server hardware from Chinese company New H3C Technologies.

This research further showcases the continued failure of multiple countries to regulate and provide transparency on the exports of surveillance technology, and the hardware that enables the use of surveillance technology which pose serious human rights risks. The companies providing exports in question should have conducted human-rights due diligence and scrutinised the human rights impacts of the deployment and maintenance of such systems, and the exporting state authorities should have scrutinised the human rights risks these exports may have posed before deciding whether to license, or otherwise allow, them. The report also shows once a technology is exported, as in the case of Sandvine, it can then be repurposed for a new censorship system. Furthermore, the report shows how the Pakistani authorities have ignored legal requirements within domestic law and repeatedly failed to obtain warrants to wiretap.

Amnesty International sent detailed questions to the government agencies and companies involved, requesting their responses to the research findings contained in this report. However, the majority of government agencies and companies did not respond by the time of publication. Of the twenty-nine entities contacted, only Niagara Networks and AppLogic Networks responded to our request for responses. The German Federal Office for Economic Affairs and Export Control (BAFA) and the Canadian Trade Controls Bureau responded to acknowledge our letter but did not answer our questions. While Datafusion Systems and Utimaco have responded to research questions sent by Amnesty International in October 2024 and their responses are reflected in this report, the companies did not provide responses to the letters detailing the findings of the report. Finally, Geedge Networks, Inbox Business Technologies Pvt Ltd, SN Skies Pvt Ltd, A

Hamson Inc, ELC Solutions, New H3C Technologies, Thales DIS., ELINC China CO Ltd and China Electronics Corporation Limited and related entities, Pakistan Mobile Communications Limited (Jazz), China Mobile Pakistan Ltd (Zong), Telenor, Ufone, Pakistan Telecommunication Company Ltd, Cyber Internet Services Pvt Ltd, Huawei, Transworld Associates, Pakistan Telecommunication Authority, Ministry of Information Technology and Telecommunications/Ignite, the Inter-Services Intelligence, the United Arab Emirates Executive Office for Control and Non-Proliferation, the Chinese Ministry of Commerce, the U.S. Department of Commerce, and the French Ministry of Economy had not responded ahead of the publication deadline. The limited responses to Amnesty International's questions to the entities involved reinforces a central theme in this report: the lack of transparency and information around the trade and deployment of surveillance and censorship technologies.

The report underscores the urgent need for stronger safeguards, greater transparency, and robust accountability mechanisms, all grounded in a human-rights based approach, to prevent the further erosion of digital and human rights in Pakistan and beyond.

**AMNESTY INTERNATIONAL
IS A GLOBAL MOVEMENT
FOR HUMAN RIGHTS.
WHEN INJUSTICE HAPPENS
TO ONE PERSON, IT
MATTERS TO US ALL.**

CONTACT US



contactus@amnesty.org



+44 (0)20 7413 5500

JOIN THE CONVERSATION



www.facebook.com/amnesty



@Amnesty

SHADOWS OF CONTROL

CENSORSHIP AND MASS SURVEILLANCE IN PAKISTAN

EXECUTIVE SUMMARY

This report documents how a range of private companies from around the world have provided, and in some cases continue to provide, surveillance and censorship technologies to Pakistan, despite Pakistan's troubling record on the protection of rights online. A lack of transparency over the sale and transfer of surveillance and censorship technologies has enabled a flourishing global trade, including exports from Canada, China, Germany, the US and the UAE to Pakistan.

The report highlights the lack of legal safeguards in Pakistan to prevent surveillance and censorship abuses, against a background of an increasingly oppressive political landscape, including the use of draconian laws to criminalize online free expression, a clampdown on protest and assemblies, arbitrary arrests and detentions and enforced disappearances. The report offers recommendations for legal reforms in Pakistan to safeguard from surveillance and censorship abuses, as well as steps the companies involved should take to meet their human rights responsibilities.