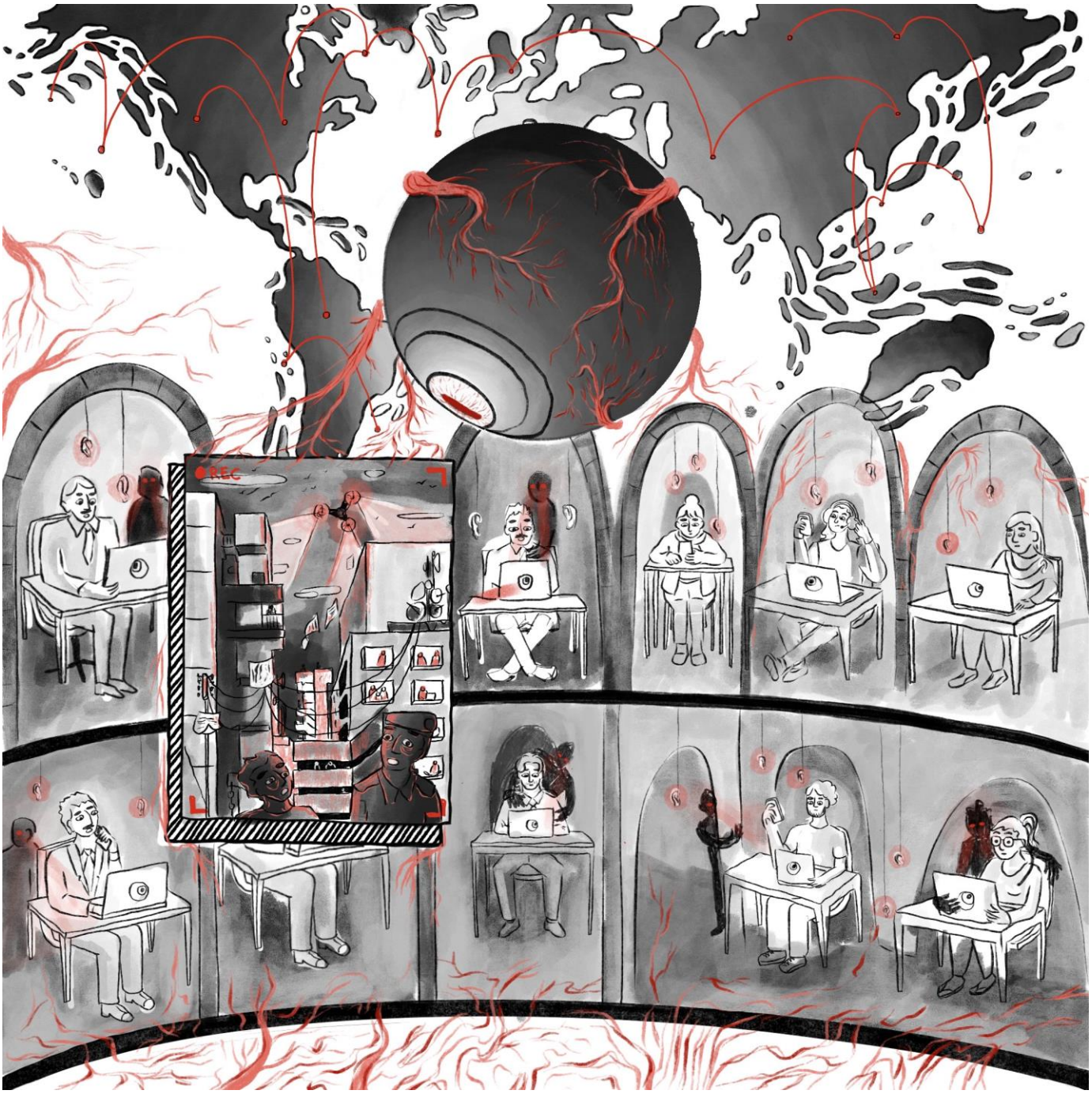


SHADOWS OF CONTROL

CENSORSHIP AND MASS SURVEILLANCE IN PAKISTAN

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.

First published in 2025
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: ASA 33/0206/2025
Original language: English

amnesty.org

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*

AMNESTY INTERNATIONAL

CONTENTS

GLOSSARY

ACTIVE FIBRE TAP	A powered device that copies network traffic to monitoring ports, often amplifying, regenerating, or aggregating signals to compensate for losses or provide advanced features. Used with both copper and fibre cabling.
BINARIES	Binaries are compiled source-code that makes it possible to run on the operating system.
CONFLUENCE	A web collaboration platform that enables teams to create, share and manage content, ideas and knowledge across the organization.
DEEP PACKET INSPECTION	Deep packet inspection (DPI) is a technique that involves examining the contents of internet protocol (IP) packets at the protocol layer, beyond just the header information. DPI enables network devices or applications to inspect and analyse the payload data within each packet, allowing for more detailed examination and classification of network traffic or the blocking of said traffic.
INTERNET PROTOCOL (IP)	A set of rules that define how data is addressed, packaged and sent across networks. It consists of two versions, IPv4 and IPv6, that assign a numerical label, called an IP-address to each device on a network, enabling devices to find and talk to each other.
JIRA	A web project management tool used by software development teams, IT organizations and other businesses to track and manage work items, issues and projects. Jira provides a suite of features for issue tracking, workflow management, and integration with other tools and services.
LAWFUL INTERCEPT	A process that enables law enforcement agencies to collect and analyse communications data from telecommunications networks, telecommunications providers or other digital services.
LAWFUL INTERCEPT MANAGEMENT SYSTEM (LIMS)	LIMS is a product sold by Utimaco, a company with headquarters in Germany. That allows for the classification of internet traffic and mobile communications such as text messaging and voice and store this data for authorities to go through.
MONITORING CENTER NEXT GENERATION (MCNG)	McNG is a product by Datafusion, formerly Trovicor, it allows authorities to sift through the material collected by LIMS. Through the McNG system operators can see whose been calling whom, when this happened, what websites were browsed, if someone might've used WhatsApp or a VPN and their location.
PASSIVE FIBRE TAP	An unpowered splitter that creates a direct, unmodified copy of network traffic. Common in fibre networks via optical splitters, and usable with copper where signal loss is acceptable.
SMOKEPING	A way to measure, store and display latency in the observed network.
TELECOMMUNICATIONS PROVIDER	A company or organisation that offers services to consumers or a business for transmitting voice, data, text, internet, sound and video over a distance. For example, through GSM wireless technology and fibre optic systems, that enables said communication between users, nationally or internationally.
TRANSPORT LAYER SECURITY (TLS)	Transport Layer Security is a method to authenticate and encrypt communication or information. Any time you use https to visit a website is when you make use of TLS.

SUMMARY OF COMPANIES

This report features a number of companies, many of which have undergone extensive renaming, change changed their corporate structure or been acquired. This table summarises the primary companies featured in the reporting and the naming conventions that Amnesty has used for readability purposes.

DATAFUSION	A group of companies including DF Systems LZ-LLC (United Arab Emirates), Datafusion Systems Gmbh (Germany), Datafusion Systems S.r.o (Czechia), and Soft Dev KL Sdn Bhd (Malaysia). Prior to 2024, the group of companies operated under the name 'Trovicor'. Where 'Trovicor' is referenced in this report, it relates to activities prior to the renaming of companies to Datafusion. Datafusion's related entity in Pakistan was not renamed and is still called Trovicor Smc Pvt Ltd. Additionally Trovicor Solutions FZ LLC, located in the UAE was not renamed. In July 2025 the Datafusion group of companies were acquired by Lumine Group (Canada). Datafusion has close ties with Utimaco.
UTIMACO	Is the tradename of the German company, Utimaco Gmbh. Utimaco creates the LIMS interception software. They have close ties with Trovicor, now Datafusion, for over a decade.
GEEDGE NETWORKS	Is the tradename of a group of Chinese companies located throughout China. The companies include, Jizhi (Hainan) Information Technology Co Ltd, Jizhi (Guangzhou) Information Technology Co Ltd and Jizhi (Chengmai) Information Technology Partnership (Limited Partnership).
SANDVINE	Sandvine was the tradename of a Canadian company that was renamed as Applogic Networks in March 2025. This report focuses on activities carried out while the company was called Sandvine, and for readability purposes uses 'Sandvine' throughout
THALES DIS	Thales DIS is part of the French defence giant Thales S.A, trading as Thales Group. Thales DIS acquired Gemalto in 2019. In this report for readability purposes, Thales DIS is used.
NIAGARA NETWORKS	Is the tradename of a U.S company that creates the fibre tap hardware used in the WMS.
TELECOMMUNICATIONS PROVIDERS IN PAKISTAN	This report documents how seven telecommunications providers in Pakistan have received shipments of surveillance and/or censorship technologies: Jazz (Pakistan Mobile Communications Limited); Zong (CMPak Limited); Telenor; Ufone; Pakistan Telecommunication Company ltd (PTCL); Cyber Internet Services Pvt Ltd; and Transworld Associates.
PAKISTANI SUPPORT COMPANIES	This report documents several Pakistani companies who have contributed to one or both iterations of the WMS: A Hamson Pvt Ltd, SN Skies Pvt Ltd, and Inbox Business Technology Pvt Ltd.
NEW H3C TECHNOLOGIES CO, LTD	Previously Hangzhou H3C Technologies Co., Ltd, now New H3C Technologies co, ltd, is a Chinese technology manufacturer that makes servers, routing/switching hardware and similar technology.
CHINESE STATE-OWNED COMPANIES	This report documents the involvement of two Chinese state-owned companies in the shipment of Geedge Network hardware: China Electronics Corporation and its subsidiary, ELINC China Co. Ltd.

ACRONYMS

WORD	DESCRIPTION
CEC	China Electronics Corporation
CEIEC	China National Electronics Import and Export Corporation
DII	Digital Information Infrastructure
DPI	deep packet inspection *(see glossary)*
ECC	Economic Coordination Committee
FIA	Federal Investigation Agency
ICCPR	International Covenant on Civil and Political Rights
IHC	Islamabad High Court
IP	internet protocol *(see glossary)*
ISI	Inter-Services Intelligence
LIMS	Lawful Intercept Management System
LLM	large language model
MOITT	Ministry of Information Technology and Telecommunications
NADRA	National Database and Registration Authority
NAT	Network Address Translation
OCR	Optical Character Recognition
OECD	Organisation for Economic Co-operation and Development
OONI	Open Observatory for Network Interference
PECA	Prevention of Electronic Crimes Act
PTA	Pakistan Telecommunications Authority
PTI	Pakistan Tehreek-e-Insaf
TSG	Tiangou Secure Gateway
VPN	virtual private network
WMS	Web Monitoring System

1. 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 Myanmar[4] 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

[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).

internet censorship 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.

2. METHODOLOGY

This report investigates the role of companies in providing surveillance and censorship technologies for import and deployment in Pakistan. The report finds that these technologies are likely to be used to target civil society and human rights in the country. For this investigation, Amnesty International worked with open-source material including commercial trade data, leaked information from Geedge Networks, and interviews with civil society and insiders at telecommunications providers.

A coalition was formed of NGOs and journalists to examine leaked documents. It included Interseclab, the Tor Project, Justice for Myanmar, Paper Trail Media and partners, the Austrian newspaper DER STANDARD and Follow The Money, The Globe and Mail and Amnesty International. The coalition searched through a total of 600GB of leaked data from Geedge Networks. This data exposes deployment of systems exported to Pakistan by Geedge Networks. This exclusive leak encompasses the company's internal Jira (a ticketing and task management system) and Confluence data (a software that allows an individual to write internal documentation and share it with coworkers) in source code and software files that Geedge uses for deployment, it was possible using the software files to get an intimate understanding of Geedge's products, all the source code was available.

Analysing a data leak of this size involved several complex steps. Most of the information was in Chinese and at times text had to be extracted from screenshots or pictures using optical character recognition (OCR). Amnesty International used a combination of OCR via Apple's Vision framework, as well as large language models (LLMs), to summarize the Jira and Confluence data and tag documents potentially relevant to the deployment of technologies in Pakistan, after having identified certain keywords. Amnesty International acknowledges error margins and conducted human review. Both the source documents and the summarized LLM documents were ingested in a full-text search system setup by InterSecLab which allowed Amnesty International to broaden its search queries in the dataset for specific keywords.

The LLMs allowed Amnesty International to select documents deemed relevant to the research and to provide English summaries[6] of the products offered by Geedge Networks. All documents directly cited in this report were translated by Chinese speakers for accuracy.

Amnesty International obtained open-source material, such as commercial trade databases on subscription-based platforms 52WMB and Sayari, showing trade data from Datafusion (formerly Trovicor) entities detailing their sales to Pakistan between 2014 and 2024. Review of these documents was supplemented by social media content from Pakistani companies providing staff to government entities deploying surveillance technologies, as well as previously published research, including Privacy International's 2015 report on surveillance in Pakistan.[7]

Amnesty International also interviewed six human rights defenders and journalists based in Pakistan about the surveillance they face and the chilling effect it has on their freedom of expression. The interviewees were contacted by Amnesty International researchers based on existing reporting of harassment and targeting by the Pakistani authorities, and the interviews were carried out online through secure platforms. These interviews were conducted in September 2024 and July 2025, at the beginning and end of the investigation. Finally, Amnesty International interviewed two sources who work for telecommunications providers in Pakistan, who were concerned about the government having such privacy-invasive access to customer data. These telecommunications provider sources were approached through trusted activist contacts inside

[6] Amnesty International used ollama and LLM models mistral:latest:7b (f974a74358d6) as well as llama3:latest:8b (365c0bd3c000).
[7] Privacy International, *Tipping the scales: Security & surveillance in Pakistan*, July 2015, https://www.privacyinternational.org/sites/default/files/2018-08/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf (accessed on 25 August 2025)

Pakistan who recommended individuals we could speak to. Interviews with telecommunications providers were conducted in February and March 2025, and all conversations were over encrypted online platforms to ensure safety of the sources. All conversations with industry workers and activists have been anonymized for security reasons.

In summary, Amnesty International was able to search and understand the dataset using a variety of digital and non-digital research methods, including LLM-supported summarizing of leaked documents, looking up Gmail accounts through open-source methods such as Ghunt which allows to see the Gmail accounts leaving Google Maps reviews,[8] searching commercial trade databases and speaking with insiders and rights-holders.

Amnesty International extends its deepest gratitude to everyone who participated in the research, in particular our research partners Paper Trail Media, InterSecLab, Justice For Myanmar, The Globe and Mail, and Tor Project. The collaboration was coordinated by Paper Trail Media, while InterSecLab provided technical support on the technical aspects of the collaboration and hosted the research platform and made the Geedge dataset searchable. Key parts of this report build upon groundbreaking recent research by InterSecLab[9] and Justice for Myanmar into Geedge Networks and its deployment in other locations[10]. Additionally, Amnesty International would like to thank FIND (find.ngo)[11] for their generous sharing of open-source information on companies and trade data and for verifying Amnesty International's obtained trade data. Amnesty International is grateful to the human rights defenders and telecommunications workers in Pakistan who shared their stories but whose names have been omitted for security reasons.

[8] GitHub, GHunt, https://github.com/mxrch/GHunt (accessed on 18 August 2025).
[9] InterSecLab report: *The Internet Coup: A Technical Analysis on How a Chinese Company is Exporting The Great Firewall to Autocratic Regimes*- https://interseclab.org/research/8
[10] Justice for Myanmar report on Geedge Networks https://www.justiceformyanmar.org/tags/geedge-networks
[11] FIND, https://find.ngo/ (accessed on 18 August 2025).

3. PAKISTAN'S USE OF SURVEILLANCE AND CENSORSHIP

3.1 HOW SURVEILLANCE AND CENSORSHIP ARE SHRINKING CIVIC SPACE IN PAKISTAN

Concerns around unlawful surveillance and online censorship in Pakistan are longstanding. Amnesty International has noted that over the past ten years, civil society in Pakistan has faced an increasingly oppressive political landscape.[12] State authorities use laws and digital technologies to restrict the rights to privacy, freedom of expression and freedom of peaceful assembly, all of which contributes to a chilling effect and a shrinking of civic space in the country. This includes a clampdown on online free speech through draconian laws,[13] arbitrary arrests and detentions, enforced disappearances,[14] targeted and mass surveillance, as well as unlawful internet restrictions.

A human rights lawyer and outspoken critic of the Pakistani authorities told Amnesty International that their devices were hacked by law enforcement authorities following their arbitrary arrest: "My phone and laptop were hacked by the agencies while I was in custody for 14 days. They even left a message on my laptop saying, 'with love, markhor' [Markhor is a logo of the ISI] and had changed my password. Obviously, that meant everything on my phone and laptop had been compromised".[15] In a follow-up interview several months later, the lawyer said they believed that their devices remained under surveillance, given the sensitive nature of the cases on which they work, including enforced disappearances, anti-terrorism charges against ethnic minorities and religious freedoms.[16]

While Pakistani law gives powers to law enforcement authorities to seize and search digital devices, a warrant for retention of any data obtained is required under local laws and authorities must inform the court of any device or data seized in connection to an ongoing case.[17] No such measure or disclosure was taken in this lawyer's case. The case underscores the ease with which safeguards such as judicial oversight in seizure and retention of data are bypassed in practice.

The Prevention of Electronic Crimes Act (PECA) was passed in 2016, placing severe restrictions on online freedom of expression and privacy. PECA uses extremely broad language to criminalize defamation, "hate

[12] Amnesty International, "Human Rights in Pakistan 2024", https://www.amnesty.org/en/location/asia-and-the-pacific/south-asia/pakistan/report-pakistan
[13] Human Rights Watch, "Pakistan: Repeal Amendment to Draconian Cyber Law", 3 February 2025, https://www.hrw.org/news/2025/02/03/pakistan-repeal-amendment-draconian-cyber-law (accessed on 25 August 2025)
[14] Amnesty International, Living Ghosts: The Devastating Impact of Enforced Disappearances in Pakistan (Index: ASA 33/4992/2021), 22 November 2021, https://www.amnesty.org/en/documents/asa33/4992/2021/en
[15] Interview over audio call with human rights lawyer, 27 September 2024.
[16] Interview over audio call with human rights lawyer, 26 February 2025.
[17] Pakistan, Pakistan Prevention of Electronic Crimes Act, ACT NO. XL OF 2016, No. F. 22(3)/2015-Legis., 22 August 2016, https://moitt.gov.pk/SiteImage/Misc/files/1472635250_246.pdf, Section 31.

speech", and "cyber terrorism".[18] The act has repeatedly been used to target journalists,[19] activists[20] and political opposition.[21]

The Pakistan Telecommunications Authority (PTA) has been granted wide and discretionary powers to block and remove content when it deems to be "in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality".[22] Further, PECA mandates that telecom companies and telecommunications providers retain "traffic data" for one year, or longer as notified by the PTA.[23] Since 2016, PECA has given legal cover to the arbitrary detention of journalists and activists[24], as well as censorship of online content,[25] including the banning of entire social media platforms from being accessed inside the country.[26] The Prevention of Electronic Crimes (Amendment) Act 2025, passed in January 2025,[27] mandates the establishment of a new agency, the Social Media Protection and Regulatory Authority, to replace the PTA.[23] This authority had not been established or notified at the time of writing. Both the current chairperson of the PTA and its previous chairperson who served from 2019 to 2023 are retired army generals,[28] indicating a nexus between the military and organisations like the PTA.

A digital media journalist from Pakistan, who was previously arrested by the Federal Investigation Agency (FIA) under PECA as a result of his journalism, told Amnesty International that following a meeting with military officials where he was warned about his social media activity, his WhatsApp account was hacked twice in two months. The journalist received an SMS code for his WhatsApp account, which he did not request, and was immediately was signed out of his WhatsApp account. Since he did not share the code with anyone, this is not normal for WhatsApp and it indicates that the code shared over mobile network was intercepted to gain access to his WhatsApp account. While it is unclear which technologies were used, the surveillance gravely affected his work. He said: "this has impacted my journalism as [now] I am always apprehensive about the safety of my sources, and it has also made sources reluctant to speak with me".[29]

Similarly, a Pakistani broadcast journalist shared with Amnesty International that "as a journalist, I know that I am under surveillance in my digital space". He added that surveillance of communications was commonly accepted as a fact among journalists: "[We know that] telecom companies in Pakistan are helping the intelligence agencies to intercept my phone calls, messages and even my movement. The PTA coordinates between intelligence agencies and telecom companies. In some instances, my WhatsApp messages were also intercepted".[30]

Most people to whom Amnesty International spoke said that their understanding of surveillance was based on instances such as leaked conversations or hacking events. Elaborating on the frequency of the surveillance he faces, the broadcast journalist said, "there were efforts to hack my email, X account and even my WhatsApp number. I know that [intelligence agencies] monitor my movements through my phone [as I am often followed]. The new surveillance methods have helped the state to silence the voices of dissent in media and civil society".[31]

---

[18] Amnesty International, "Pakistan: Repeal amendment to draconian cyber law," 28 February 2022, https://www.amnesty.org/en/latest/news/2022/02/pakistan-repeal-draconian-cyber-crime-law

[19] Al Jazeera, "'Chilling pattern': Pakistani journalists 'targeted' by cyber law", 2 November 2021, https://www.aljazeera.com/news/2021/11/2/pakistan-journalists-targeted-cyber-crime-law-press-freedom (accessed on 25 August 2025)
Freedom Network, "PECA Law Proving Dangerous For Freedom Of Expression & Journalists", 8 April 2024, https://www.fnpk.org/peca-law-proving-dangerous-for-freedom-of-expression-journalists

[20] Dawn, "Rights activist Jalila Haider booked under Peca for 'supporting BYC'", 28 April 2025, https://www.dawn.com/news/1907072 (accessed on 25 August 2025)
Dawn, "Journalists, vloggers among 150 booked under Peca", 14 December 2024, https://www.dawn.com/news/1878648 (accessed on 25 August 2025)

[21] Dawn, "PTI supporter sentenced to 3 years in prison for tweeting against army, senior military leadership", 16 February 2023, https://www.dawn.com/news/1737472 (accessed on 25 August 2025)
Dawn, "PTI activist gets 26-month jail for sedition", 23 February 2023, https://www.dawn.com/news/1738585 (accessed on 25 August 2025)

[22] Pakistan, Prevention of Electronic Crimes Act, 2016, Section 37 (now replaced by new section under 2025 amendments).

[23] Pakistan, Prevention of Electronic Crimes Act, 2016, Section 32.

[24] Amnesty International, "Pakistan: Repeal amendment to draconian cyber law," 28 February 2022, https://www.amnesty.org/en/latest/news/2022/02/pakistan-repeal-draconian-cyber-crime-law

[25] Pakistan, Pakistan Prevention of Electronic Crimes Act, ACT NO. XL OF 2016, No. F. 22(3)/2015-Legis., 22 August 2016, https://moitt.gov.pk/SiteImage/Misc/files/1472635250_246.pdf, Section 37. (accessed on 25 August 2025)

[26] Amnesty International, "Pakistan: Civil Society Joint Statement Responding to Network Shutdowns and Platform Blocking," 15 March 2024, https://www.amnesty.org/en/documents/asa33/7834/2024/en

[27] Amnesty International, "Pakistan: Authorities pass bill with sweeping controls on social media," 24 January 2025, https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/

[28] Pakistan Telecommunications Authority, "Ex-Chairmen", https://www.pta.gov.pk/category/ex-chairmen-113118101-2023-05-30 (accessed on 25 August 2025)

[29] Interview through written responses with broadcast journalist, 26 September 2024.

[30] Interview through written responses with broadcast journalist, 26 September 2024.

[31] The interviewee noted unusual activity, such as codes being generated for those accounts that were not requested by him. Interview through written responses with broadcast journalist, 26 September 2024.

A Baloch human rights defender based in Balochistan province[32] told Amnesty International: "[F]or the past few months since the crackdown intensified [against Baloch activists], I have stopped using my SIM for fear of being [forcibly] disappeared or arbitrarily detained."[33] Referring to a crackdown on protests by Baloch activists,[34] and a series of arbitrary detentions since March 2025,[35] she noted that the authorities repeatedly approach her family members and fellow organizers to make contact with her over the phone in order to trace her whereabouts. "They [the authorities] told my family that if I turn on my phone for even a few minutes they will be able to trace my location and will pick me up. They also warned that phones of all my family members are being traced in hopes that they will lead them to me."[36] No warrant for arrest or request for information has been presented in court against her, strongly suggesting that this surveillance is taking place without judicial oversight.

Another journalist, working in print and digital media, told Amnesty International he also believed he was under constant surveillance: "Obviously, everything is monitored, be it email or calls."[37] He said that, after publishing a story on corruption, he came under severe surveillance that affected him and those around them. "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? [The authorities] can go to these extreme lengths... now I go months without speaking to my family [for fear they will be targeted]."[38] He also suspected that there was close monitoring of his whereabouts and location through digital devices. He described the effect of this monitoring on his work: "As a journalist the totality of your focus should be your work, reporting the truth, but when something like this happens you start to think more about your safety."[39]

Surveillance has also been used to target state institutions such as the judiciary and government officials, including prime ministers. In a landmark 1997 judgment, the Supreme Court of Pakistan found former Prime Minister Benazir Bhutto guilty of deploying phone-tapping and eavesdropping techniques against political opponents and members of the judiciary.[40] The Supreme Court held that interception of electronic communications was a violation of Article 14 of the Constitution of Pakistan, which guarantees the right to privacy. The ruling stated that any abridgment of the right to privacy must be subject to law and judicial oversight.[41] The Supreme Court, however, did not declare section 54 of the Pakistan Telecommunication (Re-Organization) Act 1996,[42] which allows for interception of calls on the basis of national security (see section 3.2.2), as justification for violating Article 14.[43] Despite the landmark judgment, accountability for surveillance by public officials has been lacking, and high-profile cases of unlawful surveillance remain common.

More than 20 years later, Supreme Court judge, Justice Syed Mansoor Ali Shah, noted in a 2020 dissenting opinion that a sitting judge, Supreme Court judge Qazi Faez Isa, had been subject to unlawful surveillance.[44] He deemed this surveillance to be unlawful and unconstitutional. Additionally, in 2022, conversations between Prime Minister Shehbaz Sharif, Pakistan Muslim League-Nawaz leader and now-Chief Minister of Punjab province Maryam Nawaz and cabinet members were leaked, leading to apprehension that the prime minister's office was "bugged".[45] While a committee was formed to investigate the incident, no conclusion of findings has been reported nor made public at the time of writing.[46] In 2024, an open letter by six judges

[32] Balochistan, the largest province in Pakistan is in the southwestern region of the country, is a restive province with an insurgency and marked by socio-political marginalization and widespread human rights violations such as enforced disappearances and extrajudicial murders. Ethnic Baloch, a minority in Pakistan, belong to the province.
[33] Interview over audio call with Baloch activist, 4 July 2024.
[34] Amnesty International, "Pakistan: Systematic attacks and relentless crackdown on Baloch activists must end", 27 March 2025, https://www.amnesty.org/en/latest/news/2025/03/pakistan-systematic-attacks-and-relentless-crackdown-on-baloch-activists-must-end
[35] Amnesty International, *Pakistan must end crackdown on Baloch human rights defenders*, Index: ASA 33/9434/2025, 28 May 2025, https://www.amnesty.org/en/documents/asa33/9434/2025/en
[36] Interview over audio call with Baloch activist, 4 July 2024.
[37] Interview over phone with print and digital media journalist, 1 July 2025.
[38] Interview over phone with print and digital media journalist, 1 July 2025.
[39] Interview over phone with print and digital media journalist, 1 July 2025.
[40] Supreme Court of Pakistan, Benazir Bhutto v. The President of Pakistan, PLD 1998 Supreme Court 388, para. 45.
[41] Supreme Court of Pakistan, *Mohtarma Benazir Bhutto v President of Pakistan*, PLD 1998 Supreme Court 388, 1997, https://www.digitalrightsmonitor.pk/wp-content/uploads/2021/01/Mohtarma-Benazir-Bhutto-vs-the-President-of-Pakistan.pdf. (accessed on 25 August 2025)
[42] Pakistan, The Pakistan Telecommunication (Re-Organization) Act, Act No. XVII of 1996, 17 October 1996, https://www.pta.gov.pk/assets/media/pta_act_consolidated_footnotes_11012022.pdf, Section 54. (accessed on 25 August 2025)
[43] Supreme Court of Pakistan, *Benazir Bhutto v Pakistan* (previously cited).
[44] Supreme Court of Pakistan, Justice Qazi Faez Isa and others v The President of Pakistan and others, Const. P. No.17 of 2019, 4 November 2020, https://www.supremecourt.gov.pk/downloads_judgements/const.p._17_2020_dissenting_note_hj11.pdf., para. 29. (accessed on 25 August 2025)
[45] Dawn, "Leaks reveal massive breach in security at PM Office", 26 September 2022, https://www.dawn.com/news/1712044 (accessed on 25 August 2025)
[46] Al Jazeera, "Why is Pakistan investigating several audio leaks from PM office?", 29 September 2022, https://www.aljazeera.com/news/2022/9/29/why-is-pakistan-investigating-several-audio-leaks-from-pm-office (accessed on 25 August 2025)

alleged that the judges were being surveilled.[47] They noted that, in 2023, hidden cameras equipped with SIM cards were found in the home of a sitting High Court judge, including the master bedroom. They wrote that "judges of IHC had been subject to illegal surveillance that violated their privacy in the most abhorrent fashion".[48]

Such cases violate the rights of not only those subject to surveillance, but also of the public at large, who, due to inadequate safeguards, including remedy and transparency, are unable to know whether or when they may be subject to surveillance, and are therefore more likely to refrain from exercising their rights. Such chilling effects flow directly from the failure of the Pakistani authorities to provide and enforce meaningful human rights safeguards, as well as the abuse of surveillance powers.

While the use of surveillance creates a chilling effect that can deter activists from participating in civil life, control of access to the internet has also increased through censorship of content and internet shutdowns, resulting in serious human rights harms.

In 2024, Pakistan saw an increase in clampdowns on the rights to freedom of expression and peaceful assembly, including in the context of protests in Kashmir against energy bill hikes,[49] farmers' protests in Punjab,[50] Baloch protests against enforced disappearances,[51] and protests by the political party Pakistan Tehreek-e-Insaf (PTI) demanding electoral accountability.[52] Widespread human rights violations such as arbitrary detention, enforced disappearances and internet shutdowns were also reported, indicating shrinking civic space.

Narratives around cyber security and warnings against "digital terrorism" are being peddled by the state as it continues to crack down on local rights activists and opposition party members for dissent and criticism of the state, especially the Pakistan Armed Forces.[53] Speaking at the Independence Day Parade in August 2024, the Chief of Army Staff, General Asim Munir, said: "For the last few years under the leadership of anti-state, foreign powers, there have been attempts to promote digital terrorism, the purpose of which is to spread despair and sow differences in the nation by using fake news and propaganda".[54]

The government has cited cyber security[55] as a justification for upgrading the national monitoring system.[56] It has also claimed that a national firewall will help enhance the country's capability to "block propaganda and unwanted content".[57] However, as seen in the testimonies above and noted by local civil society in Pakistan, there is a clear pattern of the authorities using national security as a pretext to curb rights.

On 16 August 2024, journalist Hamid Mir filed a petition to seek redress for the violations of citizens' fundamental rights due to the alleged installation of a national firewall that drastically reduced internet speeds and resulted in routine network disruptions.[58] The Islamabad High Court (IHC) sought responses from the government and the PTA, but the case has not been listed for hearing since.

There has been little transparency from the Pakistani authorities regarding the national firewall, which has enabled internet shutdowns and censorship (see section 3.3 below). There have been repeated allegations by the public that the firewall is responsible for persistently inaccessible content on mobile internet and

[47] Dawn, "IHC judges detail 'brazen meddling' in letter to Supreme Judicial Council", 27 March 2024, https://www.dawn.com/news/1824028 (accessed on 25 August 2025)
[48] Text of the public letter reviewed by Amnesty International.
[49] BBC, "Four dead in protests against flour and energy prices", 14 May 2024, https://www.bbc.com/news/articles/c4n11j4wewxo (accessed on 25 August 2025)
[50] Dawn, "Scores held in Punjab for protesting govt's 'unfair' wheat policy", 30 April 2024, https://www.dawn.com/news/1830526 (accessed on 25 August 2025)
[51] Amnesty International, "Pakistan: Amnesty International condemns harassment faced by Baloch protestors in Islamabad", 24 January 2024, https://www.amnesty.org/en/latest/news/2024/01/pakistan-amnesty-international-condemns-harassment-faced-by-baloch-protestors-in-islamabad/
[52] Amnesty International, "Pakistan: Urgent and transparent investigation needed into deadly crackdown on opposition protesters", 27 November 2024, https://www.amnesty.org/en/latest/news/2024/11/urgent-and-transparent-investigation-needed-into-deadly-crackdown-on-opposition-protesters/
[53] Dawn, "Army chief General Asim Munir sees foreign hand in 'digital terrorism'", 14 August 2025, https://www.dawn.com/news/1852174
[54] Dawn News English, Full Speech: COAS Pakistan Addresses 'Azadi Parade 2024' At Kakul Dawn News English, 14 August 2024, https://www.youtube.com/watch?v=4fIPc8aWW8Y (accessed on 25 August 2025)
[55] Dawn "Reports suggesting internet being throttled by govt 'completely false': IT minister," 18 August 2024, https://www.dawn.com/news/1853078 (accessed on 25 August 2025) (accessed on 25 August 2025)
[56] Dawn, "Reports suggesting internet being throttled by govt 'completely false': IT minister", 18 August 2024, https://www.dawn.com/news/1853078 (accessed on 25 August 2025) (accessed on 25 August 2025)
[57] Arab News, "Pakistan's new national firewall to target 'propaganda and unwanted content,' confirms official", 30 June 2024, https://www.arabnews.com/node/2540666/pakistan (accessed on 25 August 2025)
[58] Dawn, "IHC seeks responses from govt, PTA over journalist Hamid Mir's plea against internet 'firewall'", 20 August 2024, https://www.dawn.com/news/1853517 (accessed on 25 August 2025)

messaging applications, and that its installation has reduced overall internet speeds.[59] Information about the national firewall was withheld as the government continued to offer shifting explanations regarding the use of monitoring and surveillance technologies.[60] Discussions around the national firewall installations were conducted in closed sessions by parliamentary standing committees.[61] Against this backdrop of denial and obfuscation, this report seeks to uncover the origins of these technologies and map their effects on human rights in Pakistan.

3.2 SURVEILLANCE AND MONITORING PRACTICES IN PAKISTAN

In recent years, unlawful surveillance in Pakistan has been conducted – and continues to be conducted – by a variety of means.[62] Previous research by Amnesty International in 2018 found that digital devices and accounts of human rights defenders in Pakistan were targeted and infected with spyware, by a network of individuals and companies with links to the Pakistani military.[63]

In practice, because of Pakistan's legal frameworks and surveillance practices, mass surveillance tools could be tracking a significant proportion of the population, or possibly even every resident's phone calls – including whom they call, when, and how often – without needing suspicion or reasonable cause.[64] As well as being a violation of the right to privacy, mass surveillance creates a chilling effect in society, whereby people are deterred from exercising their rights, both online and offline.[65]

3.2.1 LAWFUL INTERCEPT MANAGEMENT SYSTEM (LIMS)

Since 2007, surveillance in Pakistan has been enabled by LIMS, a product of the German company Utimaco.[66] The Pakistan Armed Forces and the Inter-Services Intelligence (ISI) use LIMS to surveil a significant portion of the population's telecoms activity through Pakistani telecoms providers, which are required under licensing agreements to comply in order to operate in Pakistan. This monitoring is conducted in the absence of a court warrant. The only information needed is a phone number, which the LIMS system then tracks. It can intercept phone calls, text messages and even internet activity and classify the traffic coming from and going to specific services, such as WhatsApp or websites visited by the target of the surveillance.[67] The PTA has reported to the IHC that telecoms providers are "under an obligation to ensure that up to 2% of their entire consumer base can be surveilled" through LIMS, meaning that more than 4 million users of telecoms services can be surveilled at any given time. Given the volume of people captured by this surveillance system, and the lack of requirements in law to disclose whose data may be collected, Amnesty International's analysis determines that the LIMS system constitutes mass surveillance. No criterion is laid out to determine which users are included in this 2%, nor have users ever been notified when subject to so-called lawful interception under LIMS. As per Amnesty International's research, the companies that supply the technology to enable LIMS and the monitoring centres to operate in Pakistan are primarily Utimaco and Datafusion.

---

[59] Amnesty International, "Pakistan: Authorities must be transparent about internet disruptions and surveillance tech", 26 August 2024, https://www.amnesty.org/en/latest/news/2024/08/pakistan-authorities-must-be-transparent-about-internet-disruptions-and-surveillance-tech/

[60] BBC, "Pakistan blames users for slow internet as firewall rumours grow", 19 August 2024, https://www.bbc.com/news/articles/cj621kk020lo (accessed on 25 August 2025)

[61] The News, "Only in-camera briefing on firewall, ministry tells Senate panel", 1 August 2024, https://www.thenews.com.pk/print/1215487-only-in-camera-briefing-on-firewall-ministry-tells-senate-panel (accessed on 25 August 2025)

[62] 'Privacy Rights Under the Lens,' Stakeholders joint submission for Pakistan's review under the third cycle of UPR, For consideration at the 28th Session UN Working Group in 2017, https://upr-info.org/sites/default/files/documents/2017-10/pi_upr28_pak_e_main.pdf (accessed on 25 August 2025)

[63] Amnesty International, *Pakistan: Human rights under surveillance* (Index: ASA 33/8366/2018), 15 May 2018, https://www.amnesty.org/en/documents/asa33/8366/2018/en

[64] Indiscriminate mass surveillance involves widespread bulk monitoring, collection, storage, analysis or other use of material and collection of sensitive personal data without individualised reasonable suspicion of criminal wrongdoing. Such collection and processing of large amounts of data is privacy violating by design and is never a proportionate interference with the rights to privacy, freedom of expression, freedom of association and of peaceful assembly.

[65] For instance, one of the activists Amnesty International spoke to pointed out that a physical assault on him, widely believed to be by the Pakistani authorities, likely took place as a result of carrying his phone with him, allowing his attackers to track his whereabouts. Others spoke of limitations on using digital communications for work, fearing that their conversations will be subject to surveillance.

[66] Privacy International, Tipping the scales (previously cited), p. 11.

[67] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan* (previously cited), para. 15 and 16.

The impact of surveillance technologies in Pakistan is augmented by the fact that government storage and control over information and data is centralized in the form of the National Database and Registration Authority (NADRA), which issues national identification cards and requires mandatory biometric registration. In Pakistan, NADRA registration is a prerequisite for accessing basic services such as healthcare and education, obtaining a SIM card and opening a back account.[68] NADRA hosts more than 228,564,529 registrations, including children, out of a population of 241 million people.[69] The centralized nature of the NADRA database and its links to large amounts of data from other databases such as electoral rolls[70] and tax registration databases,[71] maintained by private and public entities, allows for comprehensive profiles of citizens to be built and accessed by Pakistani authorities, undermining the right to privacy.[72] Amnesty International has previously found that digital identity systems, even when intended for other purposes such as social surveillance,[73] can lead to digital welfare surveillance, in a range of international contexts.[74]

Pakistan has had mandatory SIM card registration requirements since 2015.[75] This requires that cards issued by telecoms providers must be registered by the user, with the data points collected being verified biometrically, through fingerprints, against NADRA's database. Failure to register a SIM card will result in the user's phone service being blocked. As of 2025, 200 million telecoms subscribers are registered in Pakistan.[76] Although the Pakistani authorities argue that SIM card registration is mandatory to tackle terrorism and fraudulent activities, the United Nations High Commissioner for Human Rights has cautioned that the biometric data collected can be used for tracking and surveillance.[77]

Mandatory SIM card registration in Pakistan is taking place in the absence of rules and regulations to protect people's data and ensure that data is not being used, matched or merged by other public and private entities. The PTA's Subscribers Antecedents Verification Regulations 2015 only make passing reference to "confidentiality of all information disclosed by Subscribers" without any recourse to remedial measures and oversight if confidentiality is violated.[78]

This enables a more pernicious form of mass surveillance as it allows the Pakistani authorities and other entities to identify and track the owner of a SIM card. Therefore, the implementation of the LIMS system within an ecosystem of unregulated technologies – biometrics and digital identification – enables an unprecedented collection and processing of large amounts of data including sensitive data which contains characteristics that could reveal ethnicity, religion and health status. The centralization or interoperability of NADRA's databases, along with laws mandating SIM card registration, raise concerns regarding the right to privacy. Authorities should seek less invasive means to achieve their digitization goals and meet the tests of necessity and proportionality set out in international human rights law. The scope of this surveillance and its interconnectedness is expected to increase with the enactment of the Digital Nation Pakistan Act 2025, which further expands the legal cover for the creation of digital identification and digital public infrastructure systems. Amnesty International has previously raised concerns that the Act and its accompanying systems could "lead to exacerbation of existing inequalities, rights violations, and environmental harms."[79]

Pakistan's current laws do not provide adequate human rights safeguards to prevent abuse of surveillance practices. Surveillance through these technologies is not subject to individualized scrutiny to ascertain reasonable suspicion, nor is it subject to independent oversight. The UN Human Rights Committee in its second periodic review of Pakistan's obligations under the International Covenant on Civil and Political Rights

[68] The Engine Room, *Digital IDs Rooted in Justice: lived experiences and civil society advocacy towards better systems*, 2022, https://www.theengineroom.org/wp-content/uploads/2022/01/Engine-Room-Digital-ID-2022.pdf, p. 24. (accessed on 25 August 2025)
[69] National Database & Registration Authority, "NADRA Statistics", https://www.nadra.gov.pk/nadraStatistics (accessed on 25 August 2025)
[70] National Database & Registration Authority, "Election Commission: Projects", https://www.nadra.gov.pk/election-commission-projects (accessed on 25 August 2025)
[71] Profit, "FBR receives provincial data to expand tax base", 23 February 2025, https://profit.pakistantoday.com.pk/2025/02/23/fbr-receives-provincial-data-to-expand-tax-base (accessed on 25 August 2025)
[72] UN Special Rapporteur on extreme poverty and human rights, Report: Digital welfare states and human rights, 11 October 2019, UN Doc. A/74/493, para. 64.
[73] Social surveillance is a term used to describe a system that can verify one's identity but it can also be leveraged by actors for discrimination and targeting of marginalized groups.
[74] Amnesty International, *Briefing: Social protection in the Digital Age* (Index: POL 40/7771/2024), 6 March 2024, https://www.amnesty.org/en/documents/pol40/7771/2024/en/, pp. 11.
[75] The Express Tribune, "Biometric system: Two-thirds of 103 million SIMs verified", 10 March 2015, https://tribune.com.pk/story/851092/biometric-system-two-thirds-of-103-million-sims-verified (accessed on 25 August 2025)
[76] The News, "Pakistan marks 200m telecom subscribers: PTA", 20 Juen 2025, https://www.thenews.com.pk/print/1322887-pakistan-marks-200m-telecom-subscribers-ptahttps://www.pta.gov.pk/category/telecom-indicatorsthe (accessed on 25 August 2025)
[77] UN High Commissioner for Human Rights, The right to privacy in the digital age, 3 August 2018, UN Doc. A/HRC/39/29, para. 14.
[78] Pakistan, Subscribers Antecedents Verification Regulations, 30 March 2015, S.R.O. 480(I)/2015, section 19.
[79] Amnesty International, "Pakistan: Amnesty International recommendations for rights-respecting Artificial Intelligence and Digital Nation Acts" (Index: ASA 33/9244/2025), 7 February 2025, https://www.amnesty.org/en/documents/asa33/9244/2025/en

(ICCPR) expressed concern about Pakistan's "increase in surveillance measures and mechanisms".[80] The analysis in this report echoes these observations, showing that Pakistani government and intelligence agencies routinely bypass legal processes to carry out unlawful surveillance.

3.2.2 THE LEGAL FRAMEWORK FOR THE USE OF SURVEILLANCE IN PAKISTAN

Pakistan's legal and political landscape has a high tolerance for digital surveillance and interception. The Pakistan Telecommunication (Re-Organization) Act 1996 grants wide powers to the federal government to authorize "any person" under section 54 "to intercept calls and messages or to trace calls... in the interest of national security".[81] The Act does not provide a definition of national security, nor does it make the powers of the federal government subject to judicial oversight. The broad nature of this law sets the stage for a legal system that vests vast and unchecked powers in the hands of government and intelligence institutions to intercept communication systems.

Section 5(1)(b) of the colonial-era Telegraph Act 1885 is also cited by the authorities to authorize the federal and provincial governments to intercept messages under instances of "public emergency, or, in the interest of the public safety".[82] Further, PECA allows for real-time collection of information by telecommunications providers if a court authorizes a designated agency under "reasonable grounds" and "for the purposes of a specific criminal investigation".[83] This real-time collection is, however, limited to seven days or less, the extension of which is subject to judicial approval.

Judicial oversight of interception powers is limited. The Investigation for Fair Trial Act 2013 was passed as part of a series of laws to provide some level of judicial scrutiny in cases of interception and surveillance. Despite the legislative intent, the law allows for "secret warrants" to be issued by judges "in chambers" as opposed to open hearings.[84] These warrants compel telecommunications providers and telecommunications providers to share information with law enforcement authorities. Non-compliance could result in a fine of up to PKR 10,000,000 (USD 35,900).[85]

Several civil society organizations have raised concerns about the broad powers conferred by the Investigation for Fair Trial Act.[86] Nevertheless, the bare minimum requirement to obtain warrants as mandated by the law is routinely ignored by the Pakistani authorities. Submissions to the IHC by the PTA in June 2024 reveal that warrants had yet to be filed under the 2013 Act, 11 years after its passage, while extra-legal surveillance remained rife.[87] Telecommunications providers employees who confirmed to Amnesty International that the Investigation for Fair Trial Act was regularly bypassed: "The Fair Trial [Act] is not followed, [the agencies] keep asking operators for IP addresses; while civilian agencies such as the FIA and police write to us officially; [intelligence agencies] don't".[88]

Pakistan does not have dedicated legislation for data protection or data privacy. Article 14 of the Constitution of Pakistan includes "privacy of home" as a fundamental right,[89] and the article has been interpreted by the Supreme Court to cover communication systems and correspondence.[90] Pakistan has also ratified the International Covenant on Civil and Political Rights (ICCPR) which guarantees protection against arbitrary or unlawful interference with "privacy, family, home or correspondence".[91] The Ministry of Information Technology and Telecommunications (MoITT) has proposed several versions of the Personal Data Protection

[80] International Covenant on Civil and Political Rights, UN Human Rights Committee, Concluding observations on the second periodic report of Pakistan, 2 December 2024. https://digitallibrary.un.org/nanna/record/4068203/files/CCPR_C_PAK_CO_2-EN.pdf?withWatermark=0&withMetadata=0&registerDownload=1&version=1, Section 44, page 12 (accessed on 25 August 2025)
[81] Pakistan, The Pakistan Telecommunication (Re-Organization) Act, Act No. XVII of 1996, 17 October 1996, https://www.pta.gov.pk/assets/media/pta_act_consolidated_footnotes_11012022.pdf, Section 54. (accessed on 25 August 2025)
[82] Pakistan, Telegraph Act, 1885, Act NO. XIII OF 1885, 22 July 1885, https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-bp8%3D-sg-jjjjjjjjjjjj, Section 5(1)(b). (accessed on 25 August 2025)
[83] Pakistan, Pakistan Prevention of Electronic Crimes Act, ACT NO. XL OF 2016, No. F. 22(3)/2015-Legis., 22 August 2016, https://moitt.gov.pk/SiteImage/Misc/files/1472635250_246.pdf, Section 38. (accessed on 25 August 2025)
[84] Pakistan, Investigation for Fair Trial Act, 2013, ACT NO. I OF 2013, No. F. 9(21)/2012-Legis., https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FqbZw%3D-sg-jjjjjjjjjjjj, Section 9. (accessed on 25 August 2025)
[85] Pakistan, Investigation for Fair Trial Act, 2013, ACT NO. I OF 2013, No. F. 9(21)/2012-Legis., https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FqbZw%3D-sg-jjjjjjjjjjjj, Section 20. (accessed on 25 August 2025)
[86] Digital Rights Foundation, Fair Trial Bill: de-alienation of civil society, 16 March 2013, https://digitalrightsfoundation.pk/fair-trial-bill-de-alienation-of-civil-society/ (accessed 14 March 2025).
[87] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan through Secretary Ministry of Interior and Secretary Ministry of Defence and others*, Writ Petition No. 2758/2023, 25 June 2024, para. 4.
[88] Interview by voice call with employee at internet service provider in Pakistan, 8 March 2025.
[89] Pakistan, Constitution of the Islamic Republic of Pakistan, 1973, Article 14.
[90] Supreme Court of Pakistan, Benazir Bhutto v. The President of Pakistan, PLD 1998 Supreme Court 388.
[91] International Covenant on Civil and Political Rights, 16 December 1966, Article 17.

Bill, with the latest public version being made available in May 2023.[92] However, civil society and industry actors have contended that the draft Bill falls short of international human rights standards.[93]

The legal structure emerging from this patchwork of legislation provides wide, unchecked powers to the federal government to authorize surveillance with little requirement for transparency or oversight. Furthermore, there are limited mechanisms to rein in these powers, and the few mechanisms that do exist are routinely bypassed by the authorities in the absence of accountability.

PECA makes unauthorized interception by technical means and "dishonest intention" an offence with imprisonment of up to two years and fine which may extend to PKR 500,000 (roughly USD 1,762 with the conversion rate of 18 August 2025).[94] However, no state institution or official has been held accountable under this offence at the time of writing, despite the widespread prevalence of interception practices.

3.2.3 LEGALIZING LIMS

In order to carry out digital surveillance or interception of communications, it is common practice for governments to pass laws that require telecommunications or technology providers to allow access for law enforcement agencies to conduct monitoring of communication on their networks. Providers may be mandated to intercept telephone calls, monitor email communications or collect other data, such as metadata, on their users. States and companies often refer to such surveillance systems and practices as "lawful interception". However, like any surveillance system, such systems are prone to abuse. The question of whether the interception they facilitate is indeed lawful depends on whether the tools used, and the specific uses they are put to, comply with international law and standards, and whether adequate legal safeguards exist to ensure that this is the case. Unlawful abuses happen when – as in Pakistan – governments or law enforcement agencies bypass legal protections to access private communications, or when legal protections are absent or inadequate.

The installation of LIMS in Pakistan was documented by Privacy International in a 2015 report, which describes it as a "mediation platform between telecommunications companies and law enforcement monitoring centres".[95] More details of the operations of LIMS were disclosed following a court case filed in 2023 after a series of prominent cases of interception and leaking of audio recordings of calls between politicians and public figures became public in the period between 2022[96] and 2023[97]. These leaks primarily related to members of the former ruling party, PTI.[98] The case, Bushra Imran Khan v Federation of Pakistan, was filed at the IHC to investigate these recordings and the legality of interception of telecoms.[99] Based on court orders, the PTA was compelled to disclose to the court that it had issued[100] directions to Telecom Licensees to "finance, import and install LIMS at a designated place for the use of designated agencies".[101]

The court documents revealed that "the entire content of communication between the consumers undertaken through the network of the Telecom Licensee, including his/her audio and video content and web page records are shared with the monitoring center at the Surveillance Center".[102] The "Surveillance Center" is a unit identified by the PTA which can be used by "designated agencies".[103] The court further

[92] Ministry of Information Technology & Telecommunication, "Draft of the personal data protection bill, 2023", https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf (accessed on 25 August 2025)
[93] Digital Rights Foundation, "Analysis: Personal Data Protection Bill 2023", 18 July 2023, https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf (accessed on 25 August 2025)
Asia Internet Coalition, "Asia Internet Coalition (AIC) Industry Submission on Pakistan Draft Data Protection Bill 2023 (Private Member Bill), Proposed Redline Changes", 8 May 2023, https://aicasia.org/download/680/ (accessed on 25 August 2025)
US Chamber of Commerce, "Submission on the Draft Pakistan Personal Data Protection Bill, 2023", 21 July 2023, https://www.uschamber.com/international/submission-on-the-draft-pakistan-personal-data-protection-bill-2023 (accessed on 25 August 2025)
[94] Pakistan, Pakistan Prevention of Electronic Crimes Act, ACT NO. XL OF 2016, No. F. 22(3)/2015-Legis., 22 August 2016, https://moitt.gov.pk/SiteImage/Misc/files/1472635250_246.pdf, Section 19. (accessed on 25 August 2025)
[95] Privacy International, Tipping the scales (previously cited), p. 14.
[96] Aaj News, "How audio leaks overshadowed major political events," 10 December 2022, https://english.aaj.tv/news/30306416/how-audio-leaks-overshadowed-major-political-events (accessed on 25 August 2025)
[97] Dawn, "As audio leaks continue to emerge, PTI renews calls for investigation," 23 April 2023, https://www.dawn.com/news/1749017 (accessed on 25 August 2025)
[98] Express Tribune, "Audio leaks reveal PTI leadership's involvement in attack on army installations," 10 May 2023, https://tribune.com.pk/story/2416009/audio-leaks-reveal-pti-leaderships-involvement-in-attack-on-army-installations (accessed on 25 August 2025)
[99] Dawn, "IHC clubs petitions of Bushra, ex-CJP's son in audio leak case," 13 September 2023, https://www.dawn.com/news/1775580 (accessed on 25 August 2025)
[100] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan* (previously cited), para. 13.
[101] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan* (previously cited), para. 15.
[102] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan* (previously cited), para. 15.
[103] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan* (previously cited), para. 15.

noted that the Surveillance Center operates "without any supervision, oversight or control".[104] Data sharing protocols were facilitated by policy directives issued by the federal government. In a policy directive issued by the Ministry of the Interior in 2004 entitled "Sharing of Information of Cellular Subscribers with Law Enforcement Agencies and Provision of CLIR Facility", it was stated that the ISI and Intelligence Bureau can obtain call details of any subscriber directly from the telecommunications provider.[105] This access is subject to few safeguards; only requirements to present a First Information Report[106] or report and "sufficient justification" are included.[107]

It remains unknown to Amnesty International whether there have been attempts by Utimaco to verify the information being uploaded to the warrant management system in Pakistan. The Utimaco LIMS product includes a warrant management system for each wiretap, making it possible to audit whether the system is being used legally. However, the IHC case revealed that Pakistani law enforcement had never requested a warrant for eavesdropping of communications through LIMS under the 2013 Investigation for Fair Trial Act.[108] Despite being aware of the court case, the German government has failed to take action to review the export permit for sensitive direct access systems to Pakistan. The human rights risks inherent in such systems have been highlighted by industry and human rights groups for years.[109]

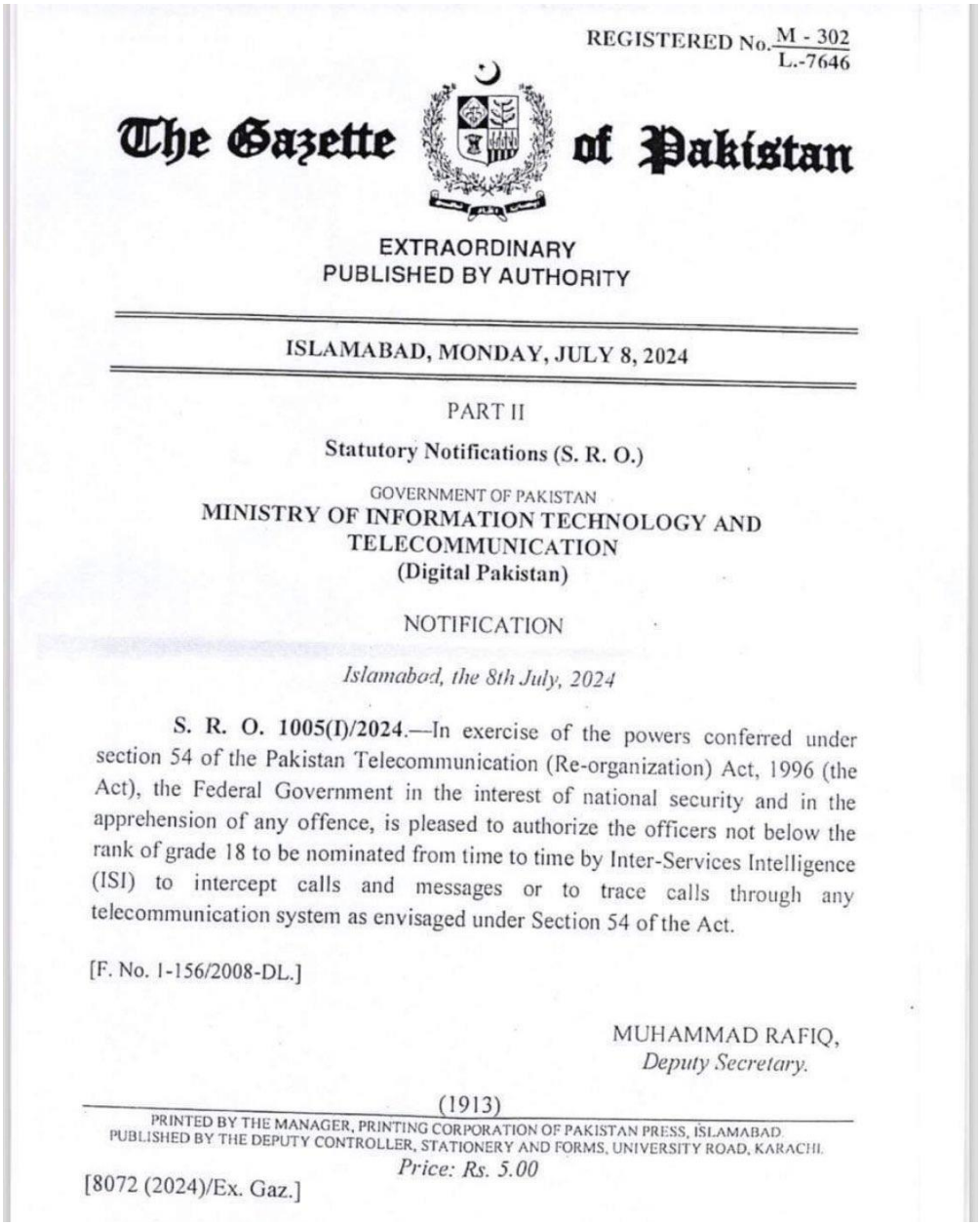
According to a document submitted to the IHC, reviewed by Amnesty International, the PTA stated that it "neither has any authority to issue instructions to enable phone tapping nor has it ever issued any directions/instructions to PTA's licensees to enable phone tapping".[110] In its order issued on 29 May 2024, the court noted that the lawyer for Pakistan-based telecoms company Pakistan Mobile Communications Limited (trade name Jazz) stated that "all telecom licensees [are] required to make infrastructure available to PTA to enable any authorized or designated agency to have access to voice and data travelling through telecom systems. Creation and provision for such infrastructure was a license requirement for all telecom licensees and the manner in which the lawful intercept infrastructure for access was created was such that even telecom licensees were unaware of its use and had no ability to monitor as to whether PTA or any authorized or designated agency was using such lawful intercept infrastructure to monitor calls or data".[111]

In light of these findings, Prime Minister Shehbaz Sharif was directed by the IHC to file a report, within six weeks of the order passed on 25 June 2024, on behalf of the federal government on whether the surveillance taking place through LIMS was legal as per the country's laws and inform the court who was responsible for the unlawful installation of LIMS and who was in charge of the surveillance system. However, the order was suspended by the Supreme Court of Pakistan on 19 August 2024 after the federal government appealed, declaring that the high court's ruling exceeded its authority.[112] The case is currently pending before the Supreme Court. Prime Minister Sharif had not made any statement on the issue at the time of writing.

In the days following these revelations in court, the Ministry of Information Technology and Telecommunications (MoITT) issued a notification on 8 July 2024,[113] authorizing ISI officers of "grade 18" or above to intercept and trace calls and messages. The notification derives its powers from Section 54 of the Telecommunications Act and provides legal cover to the ISI to intercept and surveil communications of any person with a mobile connection registered in Pakistan without any transparency, independent oversight or accountability. The notification, although challenged at the Lahore and Islamabad High Courts respectively, remains operational.[114]

---

[104] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan* (previously cited), para. 16.
[105] Ministry of Interior, 'Sharing of Information of Cellular Subscribers with Law Enforcement Agencies and Provision of CLIR Facility,' 21 September 2004, No.3/30/2003-Poll.I(1), section 5.
[106] A First Information Report (FIR) is the first step to initiating a criminal investigation. It is the official written document prepared by the police when they receive information about a criminal offence.
[107] Pakistan Telecommunication Authority, "SOP on Sharing of Information of Cellular Subscribers with Law Enforcement Agencies and Provision of CLIR Facility," 27 October 2008, No.6-10/2008/Enf/PTA.
[108] Islamabad High Court, *Bushra Imran Khan v Federation of Pakistan* (previously cited), para. 4.
[109] Amnesty International, *South Sudan: "These walls have ears": The chilling effect of surveillance in South Sudan* (Index: AFR 65/3577/2021), 2 February 2021, https://www.amnesty.org/en/documents/afr65/3577/2021/en; Privacy International, *Privacy International uncovers widespread surveillance throughout Central Asia, exposes role of Israeli companies*, 20 November 2014, https://privacyinternational.org/press-release/1186/privacy-international-uncovers-widespread-surveillance-throughout-central-asia (accessed on 25 August 2025)
[110] Letter by Pakistan Telecommunication Authority, Committee Report in response to Coordination Division letter no: PTA/Coord/Coord/875/2023 obtained by Amnesty International.
[111] Pakistan, Bushra Imran vs. Federation of Pakistan, Writ Petition No. 2758/2023, Order Sheet, 14 March 2023, para. 3.
[112] Dawn, "SC suspends IHC order in audio leaks case, bars court from further proceedings", 19 August 2024, https://www.dawn.com/news/1853303 (accessed on 25 August 2025)
[113] SRO 1005(I)/2024, 8 July 2024.
[114] Express Tribune, "Govt's surveillance order challenged in LHC", 11 July 2024, https://tribune.com.pk/story/2478709/govts-surveillance-order-challenged-in-lhc; Dawn, "Senior lawyers challenge ISI's surveillance powers in IHC", 12 July 2024, https://www.dawn.com/news/1845339 (accessed on 25 August 2025)



REGISTERED No. M - 302
L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, MONDAY, JULY 8, 2024

PART II

Statutory Notifications (S. R. O.)

GOVERNMENT OF PAKISTAN
MINISTRY OF INFORMATION TECHNOLOGY AND TELECOMMUNICATION
(Digital Pakistan)

NOTIFICATION

Islamabad, the 8th July, 2024

S. R. O. 1005(I)/2024.—In exercise of the powers conferred under section 54 of the Pakistan Telecommunication (Re-organization) Act, 1996 (the Act), the Federal Government in the interest of national security and in the apprehension of any offence, is pleased to authorize the officers not below the rank of grade 18 to be nominated from time to time by Inter-Services Intelligence (ISI) to intercept calls and messages or to trace calls through any telecommunication system as envisaged under Section 54 of the Act.

[F. No. 1-156/2008-DL.]

MUHAMMAD RAFIQ,
Deputy Secretary.

(1913)

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER, STATIONERY AND FORMS, UNIVERSITY ROAD, KARACHI.
Price: Rs. 5.00

[8072 (2024)/Ex. Gaz.]

Notification by the MoITT, dated 8 July 2024.

Amnesty International's conversations with employees from internet and telecoms service providers reveal that judicial oversight of intercept and surveillance systems is almost completely absent. A legal mosaic of licensee agreements and blanket protections for national security allow for use of intercept systems without any transparency or due process.

The intercept system in Pakistan is enforced at the telecommunications provider level through licensing agreements signed by telecommunications providers with the PTA. A template of a licence agreement provided on the PTA website notes under the National Security section that telecommunications providers "shall provide and extend at its own cost suitable equipment at premises designated by the [PTA] in consultation with the Designated Agency for the purpose of [lawful intercept]... compliant with ETSI LI and other related security standards of communications security" prior to launch of commercial operations provided by the telecommunications provider.[115] No telecommunication nor service provider can operate in the country legally without installing a lawful intercept system. Further, all telecommunications providers are

[115] PTA, "Mobile Cellular License issued under section 21 of the Pakistan Telecommunications (Re-Organization) Act, 1996, https://www.pta.gov.pk/assets/lic_template_annex-f_im_05082021.pdf. (accessed on 25 August 2025)

required to install monitoring systems that can ensure "web site/URL blocking, subject to justified technical limitation".[116] These agreements obligate all licensees to "take reasonable measures... to safeguard its Licensed System from unauthorized interception of communication".[117] However no standards are laid out, nor are any safeguards against government requests for interception.

An employee of a telecommunications provider in Pakistan, speaking to Amnesty International, shared that intercept systems are built into the basic internet service infrastructure: "[I]n order for a licensee to operate in Pakistan they have to install the system [required by the PTA]. It is only then do they get a commencement certificate and clearance from law enforcement agencies to operate in Pakistan".[118] An employee of a telecommunications provider stated that "we cannot refuse requests for information if they come from the military".[119]

3.2.4 THE ONGOING THREAT OF DIGITAL SURVEILLANCE IN PAKISTAN

Longstanding concerns regarding unlawful surveillance in Pakistan have not been addressed. Pakistan's so-called lawful intercept system builds absolute data sharing requirements into telecommunications providers infrastructure through licensing agreements and standard operating procedures that allow for data sharing at a mass level without any oversight, particularly independent and impartial judicial review of surveillance activity. The UN Human Rights Committee requires states to have authorities within the legal system entitled to exercise control over interference "with strict regard for the law".[120] The glaring lack of judicial oversight within Pakistan's surveillance systems could be seen as amounting to "arbitrary interference" under the ICCPR.[121]

Real-time surveillance under PECA, interception powers under the Telecommunications Act, secret warrants under the Investigation for Fair Trial Act, and standard operating procedures for service providers allow for law enforcement and intelligence officers to request data on broad grounds of national security. There is minimal judicial oversight within the system, and the current system under LIMS undercuts the limited judicial oversight that exists. Pakistan's international human rights commitments require that any interference with the right to privacy be consistent with the principles of "legality, necessity and proportionality".[122] Mass surveillance systems such as LIMS contravene international human rights standards "as an individualized necessity and proportionality analysis would not be possible in the context of such measures".[123]

Telecommunications providers are bound to install LIMS as a prerequisite of their licensing in order to operate in the country. The surveillance-by-design operation provides the Pakistani authorities with immense powers to access personal data and intercept information. Telecommunications providers and even the regulator, PTA, have little power to control the surveillance system once in place. The United Nations High Commissioner for Human Rights has stated that systems such as LIMS that require mandatory third-party data retention do not meet the principles of international human rights law as they appear to be "neither necessary nor proportionate".[124]

Pakistan's legal system also lacks avenues for effective remedy for individuals whose right to privacy has been violated by unlawful or arbitrary surveillance. While the Investigation for Fair Trial Act prohibits and punishes "unauthorized surveillance or interception" with up to three years' imprisonment, there is often no way of knowing if one has been subject to unauthorized surveillance by the Pakistani authorities. International human rights law requires that remedies for violations of privacy through digital surveillance should be known, accessible, and involve prompt, thorough and impartial investigation.[125] The opacity through which LIMS operates allows for surveillance without a court order, and provides effective impunity to state and intelligence agencies by creating a surveillance 'black box' within the surveillance centres. Those under surveillance are not provided notice, even after the fact, and by extension are denied an opportunity to challenge such surveillance or receive redress.

---

[116] PTA, "Mobile Cellular License", para. 6.7.10.
[117] PTA, "Mobile Cellular License", para. 7.6.2.
[118] Interview by voice call with employee at telecommunications provider in Pakistan, 8 March 2025.
[119] Interview by voice call with employee at telecommunications provider in Pakistan, 11 February 2025.
[120] UN Human Rights Committee (UNHRC), General Comment 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17), 8 April 1988, UN Doc. HRI/GEN/1/Rev.1, para. 6.
[121] UNHRC, General Comment 16 (previously cited), para. 4.
[122] UNHRC, Resolution 34: *The right to privacy in the digital*, adopted on 22 March 2017, UN Doc. A/HRC/34/L.7/Rev.1, para. 2.
[123] UN High Commissioner for Human Rights (OHCHR), Report: *best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism*, 21 July 2016, UN Doc. A/HRC/33/29, para. 58.
[124] OHCHR, Report: *The right to privacy in the digital age*, 30 June 2014, UN Doc. A/HRC/27/37, para. 26.
[125] OHCHR, Report: *The right to privacy in the digital age* (previously cited), para. 40-41.

3.3 EXPANSIVE POWERS: RESTRICTIONS ON INTERNET ACCESS IN PAKISTAN

Authorities in Pakistan routinely use laws and digital technology to censor the internet. This includes slowing down and controlling internet speeds, shutting down the internet altogether, or monitoring and blocking content such as URLs.

As noted above, the PTA and the legally constituted but yet to be established Social Media Protection and Regulatory Authority under the Pakistan Electronic Crimes (Amendment) Act 2025 have wide powers to remove and block content under sections 37 and 2R respectively.[126]

In 2024 the PTA reported having blocked more than 1.4 million URLs since PECA was passed in 2016, and 109,771 URLs were blocked during the financial year 2023-2024.[127] Out of these 109,771 URLs, the majority were blocked for reasons of "morality" (55,723), "national security" (33,634), and incitement of hate on the basis of religion (13,422).[128] No precise definitions of these terms are provided under the law. In its reports, the PTA has claimed to have processed 75,393 URLs for blocking in 2023,[129] and 1,191,050 in 2022.[130]

The process of blocking and removing content is marked by opacity and arbitrariness. Amnesty International has noted that individual users are rarely provided any notice by the PTA, often learning that content is blocked when they are unable to access it. Moreover, no opportunity is provided to users whose content is blocked to challenge these actions. Amnesty International reviewed a notice provided by the PTA to a journalist whose website was blocked in 2024. In the notice, the PTA cited the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021[131] as the legal basis for blocking their platform.[132] The Rules were issued under section 37 of PECA, which deals with so-called unlawful online content. The Rules were subject to constitutional challenges in various courts across Pakistan,[133] particularly for violating Article 19 of the Constitution, which guarantees freedom of speech and expression, and for rulemaking beyond the scope provided under PECA.[134] These legal challenges have not resulted in the rules being struck down or de-notified. Nevertheless, the IHC referred them to parliament for review in 2022.[135] NO such review has taken place at the time of publishing.

The Pakistani authorities have also attempted to use court orders as legal basis to compel social media platforms to block content. In July 2025, 27 owners of YouTube channels, many of whom where journalists, received notices from YouTube alerting them that a judicial magistrate in the capital, Islamabad, had issued an order requiring the blocking of their YouTube channels.[136] The order noted that the court was "convinced" that "offences punishable under the Prevention of Electronic Crimes Act and Penal Laws in Pakistan" had occurred, without specifying which offences or what content on these channels had violated

[126] Pakistan, Prevention of Electronic Crimes Act, ACT No, XL Of 2016, No. F. 22(3)/2015-Legis., 22 August 2016, https://www.nr3c.gov.pk/peca16.pdf, Section 37; Pakistan, *Pakistan Electronic Crimes (Amendment) Act, 2025*, ACT NO. II OF 2025, No. F. 9(05)/2025-Legis., 29 January 2025, https://www.senate.gov.pk/uploads/documents/1738226500_897.pdf, Section 2R. (accessed on 25 August 2025)

[127] Pakistan Telecommunications Authority, *Annual Report 2024*, December 2024, https://www.pta.gov.pk/assets/media/2024-12-16-pta_annual_report.pdf, https://www.pta.gov.pk/assets/media/2024-12-16-pta_annual_report.pdf, pp. 57. (accessed on 25 August 2025)

[128] ARY, "PTA blocks over 1.4mln sites for illegal activities under PECA", 18 December 2024, https://arynews.tv/pta-blocks-over-1-4mln-sites-for-illegal-activities-under-peca (accessed on 25 August 2025)

[129] Pakistan Telecommunications Authority, *Annual Report 2024*, December 2023, https://www.pta.gov.pk/assets/media/pta_annual_report_12022024.pdf, pp. 57. (accessed on 25 August 2025)

[130] Pakistan Telecommunications Authority, annual report 2022, https://www.pta.gov.pk/assets/media/pta_annual_report_2022_10012023.pdf (accessed on 25 August 2025)

[131] The gazette of Pakistan from 13 October 2021, ministry of information technology and telecommunication. Notification of "Removal and Blocking of Unlawful Online Content (procedure, oversight and safeguards) rules 2021" https://web.archive.org/web/20250523151035/https://www.pta.gov.pk/assets/media/removal_blocking_unlawful_content_rules_2021_2010 2021.pdf (accessed on 25 August 2025)

[132] Pakistan, Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021, SRO 1343(I)/2021, https://moitt.gov.pk/SiteImage/Misc/files/Removal%20Blocking%20of%20Unlawful%20Online%20Content%20Rules%202021.PDF (accessed on 25 August 2025)

[133] Express Tribune, "Controversial PECA act challenged in Supreme Court", https://tribune.com.pk/story/2526500/controversial-peca-act-challenged-in-supreme-court (accessed on 25 August 2025)

[134] Aaj News, "IHC seeks opinion on new social media rules", 22 November 2021, https://www.aaj.tv/news/30271913 (accessed on 25 August 2025)

[135] Dawn, "Court refers social media rules to NA speaker for review", 12 May 2022, https://www.dawn.com/news/1689194 and Islamabad High Court, Muhammad Ashfaq Jutt v. Federation of Pakistan, W.P. No.3028/2020, 11 May 2022, https://mis.ihc.gov.pk/attachments/judgements/121240/3/17-05-2022_Ashfaq_Jutt_637885690215833788.pdf (accessed on 25 August 2025)

[136] Al Jazeera, "Pakistan seeks YouTube ban on 27 opposition and journalist channels", 9 July 2025, https://www.aljazeera.com/news/2025/7/9/pakistan-seeks-youtube-ban-on-27-opposition-and-journalist-channels (accessed on 25 August 2025)

these offences. Amnesty International spoke to some of the journalists named in the order, who confirmed that they had never been made party to the case, nor were they given notice prior to the order being brought to their attention. In fact, they had found out about the court order only after YouTube had alerted them via email. The orders were subsequently challenged at the district court level and stay orders were obtained against the implementation of a possible ban on the YouTube channels.[137]

Additionally, the 2025 PECA amendments add another category of "unlawful or offensive online content". This includes any online content that is against the "ideology of Pakistan", "incites the public to violate the law", is "fake", "false" or "contains aspersions" against members of the judiciary, parliament, provincial assemblies or armed forces.[138] These powers are in addition to the already wide powers under section 37 of PECA, which empower the government authorities to block or remove content in the interest of the "glory of Islam", the "integrity, security or defence" of Pakistan, "public order", or "decency or morality."[139] They are also in addition to the 2021 Rules, which ascribe definitions from the Pakistan Penal Code 1860 and the Code of Criminal Procedure 1898 to the criteria in section 37.[140]

The ever-expanding and overlapping criteria used for online content removal and censorship in Pakistan appears to lack compliance with international human rights law. Article 19(3) of the ICCPR lays down a three-part test for restrictions placed on the right to freedom of expression. Any restriction must be provided by law, serve a legitimate aim, and be necessary and proportionate. The breath of the criteria laid down in sections 2R and 37 of PECA provide wide and discretionary powers to regulatory authorities to block and remove content. Several elements of the criteria laid down under the sections raises concerns under international human rights law.

The vagueness in language of these provisions does not meet the criteria of precision, allowing for unfettered discretion in censoring online content.[141] This is especially problematic with regards to criteria for content removal such as "offensive." It is well established under international human rights law that freedom of expression embraces expression that "may be regarded as deeply offensive" and especially given the inherent subjectivity of the term, using this as a justification to remove content will lead to violations of the right to freedom of expression.[142] Further, the definition of public order and "integrity or defence of Pakistan" draw on chapters XIV and VI of the Pakistan Penal Code which incorporates definitions from offences such as a colonial-era sedition offence (section 124-A), which was struck down by the Lahore High Court in 2023 due to its incompatibility with human rights.[143] The offence nevertheless continues to be used to silence and criminalize dissent in Pakistan, including in online spaces.[144] The chapters also include vague offences such as "public nuisance" (section 290) and obscenity (sections 292-294).

The Human Rights Commission of Pakistan, in its 2025 report on the PECA amendment, notes that the authority vested with powers of removing content lacks independence as its chairperson and members are appointed by the federal government.[145] While the law does allow for appeals against decisions regarding content removal to Social Media Protection Tribunals (section 2V), these tribunals have yet to be established. It its analysis of the amendment, Digital Rights Foundation, a local civil society organization, raised questions regarding the independence of these tribunals.[146]

Virtual private networks (VPNs) are widely used in Pakistan to circumvent restrictions on accessing content by encrypting internet traffic and routing it through servers in other countries. VPNs can act as an anonymizing tool for those engaging in dissent on the internet, particularly political dissidents, human rights defenders and journalists.[147] The PTA has attempted to block "unregistered" VPNs in Pakistan.[148] However,

---

[137] Dawn, "Islamabad court halts banning of 5 more YouTube channels", 12 July 2025, https://www.dawn.com/news/1923736 (accessed on 25 August 2025)
[138] Pakistan, Pakistan Electronic Crimes (Amendment) Act, 2025, section 2R.
[139] Pakistan, Pakistan Electronic Crimes Act, 2016, section 37(1).
[140] Pakistan, Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021, Rule 3.
[141] UNHRC, General Comment 34, para. 25.
[142] UNHRC, General Comment 34, 12 September 2011, UN Doc. CCPR/C/GC/24, para. 11.
[143] Al Jazeera, "Pakistani court strikes down sedition law in win for free speech", 30 March 2023, https://www.aljazeera.com/news/2023/3/30/pakistani-court-strikes-down-sedition-law-in-win-for-free-speech. (accessed on 25 August 2025)
[144] Arab News, "Pakistan charges Baloch activist with 'terrorism'", 23 March 2025, https://www.arabnews.com/node/2594587/pakistan Dawn, "25 protesters held as police break up BYC rally in Lyari", 19 January 2025, https://www.dawn.com/news/1886126/25-protesters-held-as-police-break-up-byc-rally-in-lyari (accessed on 25 August 2025)
[145] Human Rights Commission of Pakistan, *Prevention of Electronic Crimes (Amendment) Act 2025*, 2025, https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2025-LWC10-PECA-Amendment-Act-2025.pdf, p. 8.
[146] Digital Rights Foundation, *The Prevention of Electronic Crimes (Amendment) Act, 2025: DRF Analysis and Recommendations*, 2025, p. 9.
[147] Amnesty International, "VPNs are a vital defence against censorship – but they're under attack", 1 August 2017, https://www.amnesty.org/en/latest/news/2017/08/vpns-are-a-vital-defence-against-censorship-but-theyre-under-attack (accessed on 25 August 2025)
[148] The News International, "How Pakistan's VPN ban undermines rights", 30 November 2024, https://www.thenews.com.pk/print/1256432-how-pakistan-s-vpn-ban-undermines-rights (accessed on 25 August 2025)

the decision was temporarily withdrawn due to lack of sufficient legal grounds.[149] The PTA noted in its annual report for 2024 that it had registered 21,677 VPNs.[150] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in 2015 that state regulation requiring licences for encryption use "may be tantamount to a ban", specifically noting that, in the case of Pakistan, the PTA's requirement of prior approval for the use of VPNs "impermissibly interfere[s] with the individual use of encryption in communications".[151]

ACCESS TO THE INTERNET: AN ENABLER OF RIGHTS

Internet shutdowns restrict many human rights, most notably the right to freedom of expression, which includes the freedom to seek, receive and impart information. Access to the internet also enables a range of other human rights including, but not limited to, the rights to freedom of association and assembly, the right to education, the right to health, the right to work, and the right to an adequate standard of living. Activities such as organizing protests, speaking freely about human rights or against government policies, and documenting and disseminating information on human rights violations can rely heavily on the ability to access the internet.

Articles 19 and 21 of the ICCPR, which Pakistan has ratified, guarantee the rights to freedom of expression and peaceful assembly. States must not block or hinder internet connectivity in relation to peaceful assemblies or to curb freedom of expression. The same applies to geo-targeted or technology-specific interference with connectivity or access to content. Further, states should ensure that the activities of telecommunications providers and intermediaries do not unduly restrict assemblies or the privacy of assembly participants.

The UN Human Rights Council has unequivocally condemned internet shutdowns in various resolutions and reports for almost a decade. The Council's 2022 report on internet shutdowns highlights that, given their indiscriminate reach and broad impacts, shutdowns very rarely meet the fundamental requirements of necessity and proportionality as set out in international human rights law and, as such, states should refrain from imposing them. The report adds that states should not ban, block or criminalize the use of encryption or circumvention tools or particular communications channels such as VPNs and should instead provide access to those tools.

To comply with its obligations under international human rights law, it is not sufficient for a state not to interfere with the exercise of freedom of expression; it is also required that the state promotes adequate conditions for the full enjoyment of the right, including by lifting any barriers that may hinder expression.[152]

3.3.1 INTERNET SHUTDOWNS

The Pakistan government has regularly resorted to different forms of internet shutdown to restrict access to information. The Supreme Court of Pakistan declared in 2020 that section 8(2)(c) of the Telecommunications Act authorizes the federal government to issue directives to suspend internet services in the country for reasons of "national security, diplomatic protocols and State functions".[153] For example, in February 2024 the authorities suspended mobile internet and networks across the country on election day. The Ministry of the Interior stated that what it called the "security measures" were "essential to maintain the law and order situation and to deal with potential threats".[154] However, at the time, Amnesty International argued that the suspension of telecoms and mobile internet services was "a blunt attack on the rights to

[149] Dawn, "PTA decides not to ban VPNs over 'lack of legal grounds'", 1 December 2024, https://www.dawn.com/news/1875860 (accessed on 25 August 2025)
[150] Pakistan Telecommunications Authority, *Annual Report 2024*, December 2024, https://www.pta.gov.pk/assets/media/2024-12-16-pta_annual_report.pdf, pp. 17. (accessed on 25 August 2025)
[151] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye," 22 May 2015, A/HRC/29/32, para. 41.
[152] Office of the UN High Commissioner for Human Rights (OHCHR), "Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights", 13 May 2022, A/HRC/50/55.
[153] Supreme Court of Pakistan, Information Technology and Telecommunications, Islamabad v. CM Pak (Pvt) Ltd., C.M.A. No.3658 of 2019, 22 April 2020, para. 5.
[154] Al Jazeera, "'Inherently undemocratic': Pakistan suspends mobile services on voting day", 8 February 2024, https://www.aljazeera.com/news/2024/2/8/inherently-undemocratic-pakistan-suspends-mobile-services-on-voting-day (accessed on 25 August 2025)

freedom of expression and peaceful assembly".[155] The authorities have also regularly imposed other limitations on access to the internet that may fall short of a full shutdown. Similarly, during the 9 May 2023 protests, mobile internet was blocked across the country for several days, as was access to social media platforms including Facebook, YouTube and X.[156]

This pattern of shutting down mobile and internet services in the name of maintaining law and order has become a regular occurrence. The Keep It On coalition is a global network of more than 334 human rights organizations from 105 countries, including Amnesty International, working to end internet shutdowns. It found that Pakistan carried out at least 77 internet shutdowns between 2016 and 2024; with 24 incidents in 2024 alone, suggesting the use of shutdowns is increasing.[157] These shutdowns include the selective blocking of specific sites or content, and 'bandwidth throttling', with the intention of slowing internet traffic. In the lead-up to the 2024 general election, platforms such as YouTube, Facebook and X were throttled on multiple occasions when the opposition party PTI held virtual rallies.[158] A week after the election, X was banned in Pakistan for 16 months on the pretext of national security.[159] Amnesty International, in a statement published with 28 other civil society organizations, noted that the ban set a troubling precedent.[160] X was unblocked on 7 May 2025,[161] in the midst of escalation of hostilities between India and Pakistan.[162]

Localized internet shutdowns are particularly common in Balochistan and Khyber Pakhtunkhwa provinces. Activists in both provinces have told Amnesty International that these shutdowns are often used to disrupt protests and political rallies. Multiple districts in these provinces experience internet and mobile network shutdowns that last for months or even years. In August 2025, the authorities announced the suspension of mobile internet services across Balochistan province purportedly due to "security concerns" and "peculiar law and order situation"[163] from 6 August till 31 August.[164] Mobile internet services were restored in the province two weeks later after an order from the Balochistan High Court,[165] after a petition was filed stating that the suspension was a violation of fundamental rights guaranteed under Pakistan's constitution, particularly Articles 9 (security of person), 15 (freedom of movement etc), 18 (freedom of trade, business and profession), 19-A (right to information) and 25 (equality of citizens).[166]

In May 2025, the Ministry of the Interior extended the internet shutdown in Panjgur district in Balochistan for a further six months due to the "prevailing security and law and order situation".[167] Internet services had already been blocked in the district for three years as per the security services.[168] Parts of the former Federally Administered Tribal Areas in Khyber Pakhtunkhwa province experienced a mobile network shutdown from 2016 to 2021,[169] and arbitrary shutdowns remain common.[170] An activist from Khyber

---

[155] Amnesty International, "Pakistan: Election-day internet shutdown is a reckless attack on people's rights", 8 February 2024, https://www.amnesty.org/en/latest/news/2024/02/pakistan-election-day-internet-shutdown-is-a-reckless-attack-on-peoples-rights (accessed on 25 August 2025)
[156] Amnesty International, "Pakistan: Authorities must show restraint and lift internet restrictions immediately", 11 May 2023, https://www.amnesty.org/en/latest/news/2023/05/pakistan-authorities-must-show-restraint-and-lift-internet-restrictions-immediately (accessed on 25 August 2025)
[157] AccessNow, "#KeepItOn: authorities in Pakistan must stop the ongoing suppression of digital rights", 12 December 2024, https://www.accessnow.org/press-release/keepiton-authorities-in-pakistan-stop-suppression-of-rights/ (accessed on 25 August 2025)
[158] Dawn, "Social media platforms across Pakistan face disruption amid PTI virtual fundraiser: Netblocks", 7 January 2024, https://www.dawn.com/news/1803919; Dawn, "Social media platforms across Pakistan face disruption amid PTI's virtual gathering: Netblocks", 17 December 2023, https://www.dawn.com/news/1798656 (accessed on 25 August 2025)
[159] Al Jazeera, "Pakistan says it blocked social media platform X over 'national security'", 17 April 2024, https://www.aljazeera.com/news/2024/4/17/pakistan-says-it-blocked-social-media-platform-x-over-national-security (accessed on 25 August 2025)
[160] Amnesty International, "Pakistan: Civil Society Joint Statement Responding to Network Shutdowns and Platform Blocking" (Index: ASA 33/7834/2024), 15 March 2024, https://www.amnesty.org/en/documents/asa33/7834/2024/en
[161] Samaa, "Pakistan lifts ban on X (Twitter) to counter India", 7 May 2025, https://www.samaa.tv/2087333073-pakistan-lifts-ban-on-x-twitter-to-counter-india (accessed on 25 August 2025)
[162] Amnesty International, "India/Pakistan: Urgent need to protect civilians amidst escalating hostilities", 8 May 2025, https://www.amnesty.org/en/latest/news/2025/05/india-pakistan-urgent-need-to-protect-civilians-amidst-escalating
[163] Dawn, "BHC orders federal, Balochistan govts to file replies on provincial internet shutdown", 13 August 2025, https://www.dawn.com/news/1930669/bhc-orders-federal-balochistan-govts-to-file-replies-on-provincial-internet-shutdown (accessed on 25 August 2025)
[164] Arab News, "Mobile internet cut across Balochistan over security threats ahead of Pakistan Independence Day", 7 August 2025, https://www.arabnews.com/node/2610973/pakistan (accessed on 25 August 2025)
[165] Dawn, "Restoration of mobile data services in Balochistan underway on BHC orders", 21 August 2025, https://www.dawn.com/news/1932301/restoration-of-mobile-data-services-in-balochistan-underway-on-bhc-orders (accessed on 25 August 2025)
[166] Express Tribune, "Internet restored in Balochistan after 15 days", 22 August 2025, https://tribune.com.pk/story/2562503/internet-restored-in-balochistan-after-15-days (accessed on 25 August 2025)
[167] Dawn, "Internet in Panjgur to remain suspended for six months", 27 May 2025, https://www.dawn.com/news/1913567
[168] Dawn, "Internet in Panjgur to remain suspended for six months" (previously cited).
[169] Dunya, "Internet services restored in district Kurram after 8 years", 28 December 2021, https://dunyanews.tv/en/Pakistan/634669-Internet-services-restored-in-district-Kurram-after-8-years (accessed on 25 August 2025)
[170] Dawn, "Residents protest suspension of internet services in Wana", 6 May 2025, https://www.dawn.com/news/1908644/residents-protest-suspension-of-internet-services-in-wana; The News International, "Waziristan residents demand restoration of internet service", 4

Pakhtunkhwa told Amnesty International that such shutdowns were often indiscriminate, but also are increasingly targeted towards stopping political mobilization.[171] Mobile network services remained inaccessible in the lead up to, and during, the Pashtun Qaumi Jirga, a political gathering organized by the Pashtun Tahaffuz Movement in October 2024.[172] The activist said, "the aim of these shutdowns is clear: to ensure that our message of the human rights violations in Khyber Pakhtunkhwa do not reach the rest of Pakistan… [The authorities] already control the print media and television channels, they use these shutdowns to ensure videos from our rallies don't reach people through social media".[173]

A Baloch activist said that it has now become common practice for the state to shut down mobile networks before and during protests and rallies.[174] Mobile network shutdown during the Baloch Raji Muchi, a political gathering organized by Baloch activists, in July 2024 lasted for 10 days, making access to and sharing of information within and outside Gwadar district virtually impossible.[175] The Baloch activist explained: "No notice is ever given before a network shutdown. In fact, whenever the internet is shut down before or during a protest, it is an indicator that a crackdown [on protesters] is about to start – the aim is to ensure that no information from here reaches people outside Balochistan".[176] She shared that, in the past, they have had to cancel online seminars on the human rights violations in Balochistan because of unexpected shutdowns. "For us, internet shutdowns are now a reality during protests. Recently we've started using walkie-talkies and making announcements from mosque loudspeakers to coordinate during protests because our mobile phones become useless."[177]

3.3.2 THE WEB MONITORING SYSTEM (WMS): PAKISTAN'S "NATIONAL FIREWALL"

In Pakistan, internet censorship is enabled by the WMS, also commonly known as Pakistan's "national firewall", which was first deployed in 2018. The WMS is primarily used to block content on the internet, including TikTok and X.[178]

The PTA described the WMS in a 2018 tender document as a "technical solution… for identifying and blocking access to any on line content classified as unlawful under PECA".[179] The WMS was supposed to be installed at the country's internet gateways, to crawl the internet with an auto-learning functionality to identify and classify 'unlawful' content. During a Senate hearing on 10 May 2018, the minister in charge of the Cabinet Division responded to questions regarding the then-yet to be acquired WMS as performing the following functions:

"Identification and eradication of grey traffic to accomplish following objectives:

i. Foreign exchange in lieu of incoming international voice traffic be remitted in the country.

ii. Traffic routed through legal means will increase operators' taxable income.

iii. To minimize security hazard as the grey call cannot be traced back.

b. Actions relating to Web Content Management can be performed by PTA under PECA-2016

2. The Contract is signed between relevant telecom operators and the vendor without involvement of public money. All LDIs (Long Distance and International), CMOs (Cellular Mobile Operators) and Submarine Cable Landing Station licensees are sharing the cost of the system under their regulatory obligations".[180]

August 2023, https://www.thenews.com.pk/print/1097075-waziristan-residents-demand-restoration-of-internet-service (accessed on 25 August 2025)

[171] Interview over phone with activist in Khyber Pakhtunkhwa, 6 July 2025.

[172] Dawn, "PTM jirga deplores militancy, sense of deprivation", 14 October 2024, https://www.dawn.com/news/1865043 (25 August 2025) Amnesty International, "Pakistan: Authorities must immediately revoke ban on Pashtun Tahaffuz Movement", 8 October 2024, https://www.amnesty.org/en/latest/news/2024/10/pakistan-authorities-must-immediately-revoke-ban-on-pashtun-tahaffuz-movement

[173] Interview over phone with activist in Khyber Pakhtunkhwa, 6 July 2025.

[174] The Diplomat, "Balochistan's Great Internet Shutdown", 25 March 2019, https://thediplomat.com/2019/03/balochistans-great-internet-shutdown

[175] Amnesty International, "Pakistan: Repeated punitive crackdowns on Baloch protests must end", 30 July 2024, https://www.amnesty.org/en/latest/news/2024/07/pakistan-repeated-punitive-crackdowns-on-baloch-protests-must-end

[176] Interview over phone with activist in Balochistan, 4 July 2025.

[177] Interview over phone with activist in Balochistan, 4 July 2025.

[178] CNN, "Pakistan bans TikTok again", 12 March 2021, https://edition.cnn.com/2021/03/12/tech/tiktok-pakistan-ban-intl-hnk

[179] https://www.pta.gov.pk/assets/media/tender_150218.pdf

[180] Senate Secretariat, "Questions for oral answers and their replies", 10 May 2019, https://www.senate.gov.pk/uploads/documents/questions/1557452708_246.pdf, p. 29.

When the PTA refers to grey traffic, it means that certain international calls are charged at local rates instead of the international rates, which they say causes the government of Pakistan to lose revenue. The PTA, from the outset identifies content management of online content as a primary function of the WMS, according to the powers granted under PECA, specifically powers to block and remove content.

3.3.3 CENSORSHIP ENABLED BY SANDVINE TECHNOLOGY: WMS 1.0

The WMS was first installed in Pakistan in 2019 using technology provided by Sandvine, a company based in Canada, as confirmed by commercial trade data and also by Coda Story journalists in 2019.[181] In this report, Amnesty International refers to the company as Sandvine; however, around 3 March 2025 it was renamed Applogic Networks.[182] Sandvine was the name under which it operated during the relevant periods under discussion in this report.

The Geedge dataset (and further described in section 4.1) shows how Pakistan updated and advanced WMS 1.0 using repurposed hardware and technologies produced by Sandvine, and new technologies produced by Chinese company Geedge Networks and shipped to Pakistan by a Chinese state-owned subsidiary, ELINC, via local subsidiaries. Amnesty refers to the second iteration of the WMS as WMS 2.0, which is described at length in section 4.1.1.

Amnesty International studied commercial trade data showing Sandvine hardware being shipped to the Pakistani company Inbox Business Technology between 2016 and 2022. This confirms the information published by Coda Story in 2019,[183] that Inbox Business Technology obtained Sandvine hardware for the Pakistani WMS. This information has not been made public by the PTA. The trade data lists show support packages in 2016 as well as Sandvine hardware and storage servers with a total declared value of USD 15 million. The true amount is likely to be higher as there is no declared value in the trade data between 2016 and 2019.

Another Pakistani company, A Hamson Pvt. Ltd. (A Hamson), also received Sandvine hardware in 2019, as revealed through trade data. While it is not clear what kind of hardware was shipped, Amnesty International confirmed that Sandvine hardware was repurposed in WMS 2.0 by A Hamson. (Please see section 4.3.1 on Geedge Networks.)

Sandvine has previously been embroiled in scandals for assisting countries in censoring access to the internet within their borders. In 2018, Sandvine was exposed by Citizen Lab for enabling countries including Egypt and Turkey to silently redirect internet users to malicious software through unencrypted HTTP links.[184] This was then used to mine cryptocurrency or inject nation-state spyware. On 28 February 2024, the US Department of Commerce added Sandvine to its Entity List, imposing strict licence requirements for exports, re-exports and transfers of US technology to Sandvine.[185] In August 2024, Bloomberg reported that Sandvine's US-based private equity owner Francisco Partners sold the company.[186]

Due to the US entity listing, Sandvine's stockpile of equipment became stuck in the USA,[187] meaning that it could not export nor install products for customers and had difficulty obtaining the necessary chips manufactured by US companies for its products. The consequences appear to have forced Sandvine to reform its corporate governance and, to a limited extent, its business practices. Commitments included no longer operating in "non-democracies or countries where the threat to digital rights is too high" and exiting 32 countries, with 24 more countries in the process of being exited. It also set up a Business Ethics

[181] Coda Story, "Pakistan moves to install nationwide 'web monitoring system'", 24 October 2019, https://www.codastory.com/authoritarian-tech/pakistan-nationwide-web-monitoring (accessed on 25 August 2025)
[182] AppLogic Networks, "Sandvine Emerges as AppLogic Networks", 3 March 2025, https://www.applogicnetworks.com/press-releases/sandvine-emerges-as-applogic-networks (accessed on 25 August 2025)
[183] Coda Story, "Pakistan moves to install nationwide 'web monitoring system'". https://www.codastory.com/authoritarian-tech/pakistan-nationwide-web-monitoring/ (accessed on 25 August 2025)
[184] Citizen Lab, "BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?", 9 March 2018, https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/ (accessed on 25 August 2025)
[185] U.S. Department of State, "The United States Adds Sandvine to the Entity List for Enabling Human Rights Abuses", 28 February 2024, https://2021-2025.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-abuses (accessed on 25 August 2025)
[186] BNN Bloomberg, "Francisco partners ends ownership of crisis-plagued Sandvine", 23 August 2024, https://www.bnnbloomberg.ca/business/company-news/2024/08/23/francisco-partners-ends-ownership-of-crisis-plagued-sandvine/ (accessed on 25 August 2025)
[187] BNN Bloomberg, "Francisco partners ends ownership of crisis-plagued Sandvine" (previously cited).

Committee for vetting new customers and identifying possible technology misuse.[188] Due to these changes, the US Bureau of Industry removed the entity listing of Sandvine on 21 October 2024.[189]

Amnesty International contacted AppLogic Networks for clarification and confirmation on the findings of this report. In a letter to Amnesty International on 22 August 2025, AppLogic Networks stated that it is independent from its predecessor Sandvine.
AppLogic Networks confirmed that "*in or around 2017, Sandvine sold hardware and software through one or more partners for use and/or deployment in Pakistan*", and acknowledged "*prior third-party misuse of Sandvine's products*", but stated that "*none of the Sandvine products were controlled for export control purposes and none had or has the capability to decrypt user data (i.e., voice, video, messaging, etc.) or inject spyware*." AppLogic Networks also stated that "*Sandvine was not aware of Geedge Networks as identified in the Amnesty International letter and any hardware repurposed as articulated in the Amnesty International letter is off-the-shelf Dell and Niagara equipment that does not contain any special capability that is unique to Sandvine's solution*."

In its letter to Amnesty International, AppLogic Networks also stated that "*Sandvine Corporation (Sandvine) has not and does not support the misuse of its products and prohibited the use of its products to violate law, regulations, and internationally recognized human rights standards, among other things*."

In its letter to Amnesty International, AppLogic Networks cited Sandvine's due process when aware of allegations of potential product misuse, and reiterated the commitments and changes made in response to the letter from civil society organisations on October 2024. AppLogic also stated that it "maintains grievance mechanisms, including one that is managed by a third party, allows for anonymous reporting, and can be used by individuals and organizations to report allegations of potential product misuse" and that it has a "clear commitment to championing human rights".

In a letter to Sandvine in October 2024, several civil society organizations, including Amnesty International, asked for more clarity on how Sandvine will try to work with civil society and with which countries it will no longer do business.[190] In its reply, Sandvine listed Pakistan among the list of countries from which it would divest.

The full letter sent by AppLogic Networks to Amnesty International on 22 August 2025 can be found in Annex 3.

Chapter 4 details Amnesty International's evidence of how new iterations of the WMS were updated using technology provided by a Chinese company, Geedge Networks.

3.3.4 LEGALITY OF CENSORSHIP AND INTERNET SHUTDOWNS IN PAKISTAN

Internet shutdowns and arbitrary blocking of content can serve as powerful markers of deteriorating human rights situations.[191] Indeed, internet censorship in Pakistan violates the human rights of everyone in Pakistan on a broad scale. Censorship of content is not subject to transparent reasoning, and there is no meaningful mechanism of redress. Deployment of the firewall and WMS to block entire social media platforms and wholesale internet shutdowns, which have included country-wide shutdowns, have failed to meet the requirements set out in international human rights law, particularly the requirement of proportionality.[192] Moreover, these shutdowns are not authorized by independent courts before being instituted.

Pakistan's current regulatory regime for blocking content and services is based on broadly defined criteria with no requirements for transparency or judicial oversight. Under the current legal regime, internet shutdowns are implemented through policy directives issued by the federal government. The PTA is required

[188] Applogic Networks, "Sandvine: Our Next Chapter as a Market Leader for Technology Solutions", 19 September 2024, https://www.applogicnetworks.com/press-releases/our-next-chapter-as-a-market-leader-for-technology-solutions (accessed on 25 August 2025)
[189] Bureau of Commerce and Industry, "Commerce Removes Sandvine from Entity List Following Significant Corporate Reforms to Protect Human Rights", 21 October 2024, https://www.bis.gov/press-release/commerce-removes-sandvine-entity-list-following-significant-corporate-reforms-protect-human-rights (accessed on 25 August 2025)
[190] Access Now, "Sandvine must make good on its commitments and stop harming human rights", 31 October 2024, https://www.accessnow.org/press-release/joint-letter-to-sandvine-on-announced-reforms (accessed on 25 August 2025)
[191] Office of the United Nations High Commissioner for Human Rights, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, 13 May 2022, A/HRC/50/55, para. 24.
[192] Office of the United Nations High Commissioner for Human Rights, Internet shutdowns (previously cited), para. 11.

to comply with these orders under section 8 of the Telecommunications Act.[193] Amid this censorship, Pakistani authorities sought to regulate use of VPNs through the requirement of registering all VPNs to be used for "commercial purposes", while threatening to block all non-commercial and unregistered usage.[194]

Pakistan's laws do not meet the requirements under Article 19(3) of the ICCPR, which states that the right to freedom of expression and access to information be restricted only in specific circumstances relating to "rights or reputations of others or to the protection of national security or of public order (ordre public) or of public health or morals". The overly broad nature of Pakistan's laws exceeds the specific restrictions provided for in the ICCPR and the three-part test, that restrictions must be provided by an accessible and precise law, for a legitimate aim and be necessary and proportionate to that aim.[195] As a result, the rights to freedom of expression and freedom of assembly are being violated in Pakistan through the deployment of technologies used for removal or blocking of content and platforms and for internet shutdowns.

Furthermore, blockage of or disruption to internet access can have a disproportionate effect on marginalized groups who may rely on the online space to access information and education, or advocate for their rights.[196] This can further exacerbate the "digital divide",[197] particularly for regions including Balochistan and Khyber Paktunkhwa where large areas are regularly cut off from internet access.[198] The frequency and vast volume of content removal requests relating to anti-state content contributes to silencing of dissent and further marginalization of communities. Shutdowns also have a devastating impact on those who rely on internet connectivity to make a living in the platform or gig economy, such as via ride-hailing and food delivery services.[199] Women, LGBTI people and other marginalized workers in this sector already face increased risks and adverse working conditions.[200]

Internet disruptions that take place during armed conflict, elections or other politically contentious events may suppress political participation, peaceful assembly and other rights.[201] Even where such effects are incidental to a legitimate purpose to block content and connectivity, they may create disproportionate human rights harms which outweigh that purpose, rendering them unlawful under international human rights law.

3.4 FUNDING FOR SURVEILLANCE AND CENSORSHIP TECHNOLOGY IN PAKISTAN

It is unclear where the funding for upgrading Pakistan's national firewall system has come from. In a Question and Answer session at the Senate Secretariat on 12 September 2024, the Minister for Information Technology and Telecommunications, Shaza Fatima Khawaja, stated that the "PTA is not involved in the funding, procurement, deployment or operations of any Firewall project at the National level".[202] Attempts by journalists to obtain information regarding its cost and where it was procured from have been met by vague answers from the PTA. At the time of writing a petition at the IHC, filed by journalist Saman Amjad, was requesting information on the WMS. Further, while procurement documents such as the "proposal for prequalification" for the WMS are available on the PTA website,[203] no documents have been shared for procurement of upgrading services.

---

[193] Pakistan, Pakistan Telecommunication (Re-Organization) Act, 1996, Act No. XVII of 1996, section 8.
[194] UN Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 4 August 2022, A/HRC/51/17, para 23.
[195] Human Rights Committee, General comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 21.
[196] The Knowledge Forum, Disconnected Nation: How Internet Shutdowns Are Choking Pakistan's Democracy and Progress, December 2024, https://www.theknowledgeforum.org/disconnected-nation-how-internet-shutdowns-are-choking-pakistans-democracy-and-progress/ (accessed on 25 August 2025)
[197] Amnesty International, *Briefing: Gender and Human Rights in the Digital Age* (Index: POL 40/8170/2024), 10 July 2024, https://www.amnesty.org/en/documents/pol40/8170/2024/en/, p. 2.
[198] Arab News, Balochistan youth swap trees for tech as Internet lab bridges digital divide, 26 June 2025, https://www.arabnews.com/node/2605865/pakistan; Khyber Pakhtunkhwa, Digital Policy, 22 November 2018, https://www.kpitb.gov.pk/sites/default/files/Khyber%20Pakhtunkhwa%20Digital%20Policy%202018-2023.pdf (accessed on 25 August 2025)
[199] Dawn, "Infrastructure: Pakistan's Internet Recession", 19 January 2025, https://www.dawn.com/news/1886098 (accessed on 25 August 2025)
[200] Amnesty International, *Briefing: Gender and Human Rights in the Digital Age* (Index: POL 40/8170/2024), 10 July 2024, https://www.amnesty.org/en/documents/pol40/8170/2024/en/https://www.amnesty.org/en/documents/pol40/8170/2024/en/, p. 24.
[201] Amnesty International, "A web of impunity, 16 November 2021", https://iran-shutdown.amnesty.org
[202] Senate Secretariat, "Questions for Oral Answers and their Replies", 342nd Session, 12 September 2024, https://senate.gov.pk/uploads/documents/questions/1726113987_736.pdf, Question No. 99. (accessed on 25 August 2025)
[203] Pakistan Telecommunications Authority, "Prequalification for Web Monitoring System", https://www.pta.gov.pk/assets/media/tender_150218.pdf (accessed on 25 August 2025)

Pakistani officials have long denied the installation of a firewall,[204] dismissing reports from media and civil society by stating the government was merely upgrading the existing WMS.[205] While officials have offered differing and shifting explanations regarding changes in users' experience of the internet in Pakistan, activists and experts have argued that WMS 2.0 is qualitatively different from the previous system[206]. The existence of the firewall was confirmed during a question-and-answer session at the National Assembly on 6 August 2025.[207] During the session, Minister for Information Technology and Telecommunication, Shaza Fatima Khawaja, claimed the firewall complied with constitutional safeguards and was essential for cybersecurity.[208]

While there is no clarity on where funding for the firewall has come from, media reports have offered some indication. Reporting by the media suggested that PKR 5 billion (USD 17,861,860) was redirected for utilization by the ICT R&D Fund, also referred to as the Ignite National Technology Fund (Ignite Fund), in November 2023 as bridge financing utilized for the firewall as part of the Digital Information Infrastructure (DII) initiative. This decision was made by the Economic Coordination Committee (ECC), which is part of the federal cabinet headed by the prime minister. It was reported by the news outlet Express Tribune that the PKR 5 billion was "diverted from the [Universal Service Fund] to the social media firewall project".[209] In February 2024, the ECC also approved a "technical supplementary grant" of PKR 10 billion (USD 35,723,740) for the DII initiative.[210] Little is known about the DII initiative, but it has been reported that it is designed to bolster cyber security capabilities,[211] providing "technical capabilities to proactively identify potential cyber threats on the national critical information infrastructure".[212] Statements made by the PTA chairperson in 2024 suggests that approval for upgrading the WMS and the firewall project was granted in March 2019,[213] but implemented later due to financial constraints.[214]

The Ignite Fund was established by the MoITT for "research and development activities in the field related to Information and Communication Technology" through a 2006 amendment to the Telecommunications Act.[215] The Ignite Fund consists of grants and loans from the federal government, contributions by licensees, and grants and endowments received from other government agencies.[216] The Research and Development Fund Rules 2006 state that the Fund would operate as a non-profit public limited company.[217] The Rules also state that "all applications for research and development grants, research findings and reports produced by the principal investigator shall be kept confidential".[218] The Fund is required, however, to maintain a public register with "brief particulars of the applications received, projects awarded, status of the projects and other relevant particulars in such form as may be decided by the Board from time to time".[219] The Act

[204] Dawn, "PTA official offers yet another reason for internet woes", 22 August 2024, https://www.dawn.com/news/1853875 (accessed on 25 August 2025)
[205] Al Jazeera, "Pakistan tests secret China-like 'firewall' to tighten online surveillance", 26 November 2024, https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance (accessed on 25 August 2025)
[206] Dawn, "PTA official offers yet another reason for internet woes", 22 August 2024, https://www.dawn.com/news/1853875 (accessed on 25 August 2025)
[207] Business Recorder, "Internet firewall: Govt defends controversial rollout in NA", 7 August 2025, https://www.brecorder.com/news/40376740 (accessed on 25 August 2025)
[208] Tech Juice, "Govt Confirms Firewall Installation Amid Internet Slowdown Concerns", 7 August 2025, https://www.techjuice.pk/govt-confirms-firewall-installation-amid-internet-slowdown-concerns (accessed on 25 August 2025)
[209] Express Tribune, "ECC defers pension cuts on legalities", 28 June 2024, https://tribune.com.pk/story/2474649/ecc-defers-pension-cuts-on-legalities (accessed on 25 August 2025)
[210] Ministry of Information and Broadcasting, "ECNEC approves uplift projects worth over Rs154b", 8 February 2024, https://moib.gov.pk/News/59997 (accessed on 25 August 2025)
[211] Express Tribune, "ECC okays Rs10b for Digital Information Infrastructure Initiative", 8 February 2024, https://tribune.com.pk/story/2455818/ecc-okays-rs10b-for-digital-information-infrastructure-initiative (accessed on 25 August 2025)
[212] The Nation, "ECC approves Rs10b TSG for Digital Information Infrastructure Initiative", 8 February 2024, https://www.nation.com.pk/08-Feb-2024/ecc-approves-rs10b-tsg-for-digital-information-infrastructure-initiative (accessed on 25 August 2025)
[213] The News, "PTA chief concedes 'firewall' being upgraded", 22 August 2024, https://www.thenews.com.pk/print/1222305-firewall-system-being-upgraded-on-govt-court-orders-pta (accessed on 25 August 2025)
[214] Express Tribune, "PTA admits setting up firewall to manage social media", 22 August 2024, https://tribune.com.pk/story/2490041/pta-admits-setting-up-firewall-to-manage-social-media (accessed on 25 August 2025)
[215] "Ignite - National Technology Fund", https://ignite.org.pk (accessed on 25 August 2025)
[216] Pakistan, The Pakistan Telecommunication (Re-Organization) Act, Act No. XVII of 1996, 17 October 1996, https://www.pta.gov.pk/assets/media/pta_act_consolidated_footnotes_11012022.pdf, 33C. (accessed on 25 August 2025)
[217] Pakistan, Research and Development Fund Rules, 28 September 2006, S. R. O. 1017(1)/2006, https://www.pta.gov.pk/assets/media/research_and_development_fund_rules_2006_24012022.pdf, section 4. (accessed on 25 August 2025)
[218] Pakistan, Research and Development Fund Rules, 28 September 2006, S. R. O. 1017(1)/2006, https://www.pta.gov.pk/assets/media/research_and_development_fund_rules_2006_24012022.pdf, section 10. (accessed on 25 August 2025)
[219] Pakistan, Research and Development Fund Rules, 28 September 2006, S. R. O. 1017(1)/2006, https://www.pta.gov.pk/assets/media/research_and_development_fund_rules_2006_24012022.pdf, section 10. (accessed on 25 August 2025)

requires that the Fund be audited, and the audited annual statement of accounts be submitted to the National Assembly each year.[220]

Neither the Ignite Fund's financial statements nor register were available publicly at the time of writing, and Amnesty International could not review them for this research. No record of a request for proposals or tender for a WMS or national firewall system could be found on the Ignite Fund's website during the years 2023 or 2024.

[220] Pakistan, The Pakistan Telecommunication (Re-Organization) Act, Act No. XVII of 1996, 17 October 1996, https://www.pta.gov.pk/assets/media/pta_act_consolidated_footnotes_11012022.pdf, 33D. (accessed on 25 August 2025)

4. COMPANIES ENABLING CENSORSHIP IN PAKISTAN

Despite longstanding concerns around unlawful internet censorship by the authorities in Pakistan – of which vendors should have been aware - our research suggests that the authorities are still able to pursue new tools for the "national firewall" from private companies, enabling them to maintain, and potentially expand, their capacity for unlawful censorship. Amnesty International research reveals that these tools are being supplied – at least in part – by Geedge Networks.

By analysing leaked documents and trade databases, Amnesty International was able to gain new insights into a commercialized version of the technology used in China's so-called Great Firewall, a comprehensive tool developed and deployed by the Chinese authorities that censors the internet for users inside China. The trade data from subscription-based trade platforms allowed Amnesty International to see that a Chinese subsidiary of a state-owned company exported hardware to a Pakistani company that was used in Pakistan's updated firewall – WMS 2.0.

As such, this section describes in detail Geedge Networks and its products, and how Geedge hardware was shipped to Pakistan by ELINC, a subsidiary of an entirely state-owned company, China Electronics Corporation. It then describes how Geedge Networks' products were deployed in Pakistan and used in conjunction with hardware and software from other companies to censor the internet.

4.1 ABOUT GEEDGE NETWORKS

Geedge Networks is the English-language name of a Chinese company, founded in 2018, that produces a commercial version of China's Great Firewall. It produces multiple products that can be used to monitor large networks, such as telecommunications providers, in a managed fashion. Geedge Networks is little-known outside of China; it first attracted international attention when the NGO Justice for Myanmar alleged in 2024 that the Myanmar government had procured technology from the company to censor the internet in Myanmar.[221]

Geedge Networks works together with the Massive and Effective Stream Analysis (Mesalab) research group, part of the Institute of Information Engineering at the Chinese Academy of Sciences.[222] Fang Binxing, who has been dubbed the "father of the Great Firewall of China" was reportedly chief scientist at both China Electronics Corporation (CEC) and Geedge Networks, according to a news article published in January

[221] Justice for Myanmar, "The Myanmar Junta's partners in digital surveillance and censorship", 19 June 2024, https://www.justiceformyanmar.org/stories/the-myanmar-juntas-partners-in-digital-surveillance-and-censorship (accessed on 25 August 2025)

[222] MESA Lab, https://web.archive.org/web/20241114010446/https://mesalab.cn/ (retrieved on 14 November 2024). (accessed on 25 August 2025)

2024.[223] The article cites a speech from Fang Binxing that asserts that Geedge Networks was founded through work for which he was responsible at CEC, as part of China's "Going Out" Belt and Road Initiative.

Additional evidence in the leaked documents show that CEC or its subsidiaries are involved in the deployment and maintenance of Geedge Networks' deployments. For example, CEC is a fully state-owned enterprise in China and active in both the military and civilian market.[224] Its subsidiaries, China National Electronics Import and Export Corporation (CEIEC) and ELINC, are mentioned when disks break and require replacement and require sign-off by CEIEC representative to be replaced or shipping servers to intermediaries to be used in the case of Pakistan WMS 2.0.

In 2017 the US Treasury alleged that CEIEC exported a national firewall to a Venezuelan state-owned telecommunications provider that controls 70% of Venezuela's internet service. The US Treasury sanctioned CEIEC, placing the company on its Specially Designated Nationals list.[225]

The Geedge dataset shows that both Geedge Networks and Mesalab share a Confluence installation for documentation, a Jira instance for customer support requests as well as a Gitlab instance to work collaboratively on source code.

The dataset also shows Mesalab students working on DPI, as well as internet censorship research such as how to block certain VPN applications or other strategies to block content or services online. These research topics are all of relevance to Geedge Networks products. The leak also contains binaries[226] of the software used on the appliances from Geedge.

The Chinese companies that make up Geedge Networks are:

- Jizhi (Hainan) Information Technology Co Ltd (积至（海南）信息技术有限公司)
- Jizhi (Guangzhou) Information Technology Co Ltd (积至（广州）信息技术有限公司)
- Jizhi (Chengmai) Information Technology Partnership (Limited Partnership) (积至（澄迈）信息技术合伙企业（有限合伙)

Both Jizhi Chengmai and Jizhi Hainan are located on the Chinese island of Hainan. Jizhi Guangzhou is operated from Guangzhou.

4.1.1 EVIDENCE OF THE PROVISION OF FIREWALL TECHNOLOGY AND A CHINESE STATE-OWNED SUBSIDIARY SENDING HARDWARE TO PAKISTAN

Documents from the Geedge dataset indicate multiple meetings occurred between Geedge Networks and various Pakistani companies and institutions in 2023, including with the Pakistan Telecommunication Authority. While no sales contracts were found in the leak itself, Amnesty International was able to independently verify that Geedge Network products were ultimately used in the country as part of the Web Monitoring System (WMS 2.0).

Amnesty International found that the Geedge Networks products were deployed in Pakistan in collaboration with another company, ELINC, a subsidiary of Chinese state-owned company China Electronics Corporation (CEC).

---

[223] Sohu, 海南省方滨兴院士工作站在海南生态软件园揭牌 [Academician Fang Binxing of Hainan Province unveiled at Hainan Ecological Software Park], 11 January 2024, https://www.sohu.com/a/751088620_121719902 (in Chinese). (accessed on 25 August 2025)

[224] The China Electronics Corporation (CEC), China Electronics Co. Ltd, and ELINC are all part of a state-owned group in China. A 2024 report issued by China Software outlined the equity structure of CEC, showing it is owned by two state bodies: the SASAC and the National Social Security Fund Council. It also confirmed that CEC is the owner of China Electronics Co., Ltd. A separate 2021 acquisition report identified China Electronics Co., Ltd as the direct owner of ELINC, completing the ownership chain. Sina, 中国软件：2024 年度向特定对象发行 A 股股票预案, [China Software: 2024 plan to issue A-shares to specific targets], 26 February 2024, https://vip.stock.finance.sina.com.cn/corp/view/vCB_AllBulletinDetail.php?stockid=600536&id=9842502 (in Chinese), (accessed on 25 August 2025)

China Electronics Corporation, 收购报告书摘要 [Acquisition Report Summary], March 2021, https://pdf.dfcfw.com/pdf/H2_AN202103141471860282_1.pdf?1615739411000.pdf (in Chinese). (accessed on 25 August 2025)

[225] Office of Foreign Assets Control, Sanctions List, https://sanctionssearch.ofac.treas.gov/Details.aspx?id=30502 (accessed on 19 August 2025). (accessed on 25 August 2025)

[226] Binaries are compiled source-code that makes it possible to run on the operating system.

The role of ELINC in exporting and deploying the Geedge Network products in Pakistan was confirmed by analysis of open-source trade data, and review of communications between representatives of ELINC and Geedge Networks involved in deploying the interception hardware in Pakistan.

NETWORK HARDWARE SHIPPED BY ELINC TO PAKISTAN

Through subscription-based trade databases, Amnesty International discovered that ELINC sent computer network hardware to the Pakistani company ELC Solutions Corp (Pvt) Limited (ELC Solutions). The descriptions of hardware sent to ELC Solutions closely match those used internally by Geedge Networks when describing product components.

ELC Solutions is a company located in Pakistan. On its website, next to a picture of the Great Wall of China, it states that the company is active in the telecommunications and military sectors. On one pages of its website ELC Solutions claims to have worked on projects for several telecommunications providers, telecommunications network hardware providers, and the Pakistani military[227].

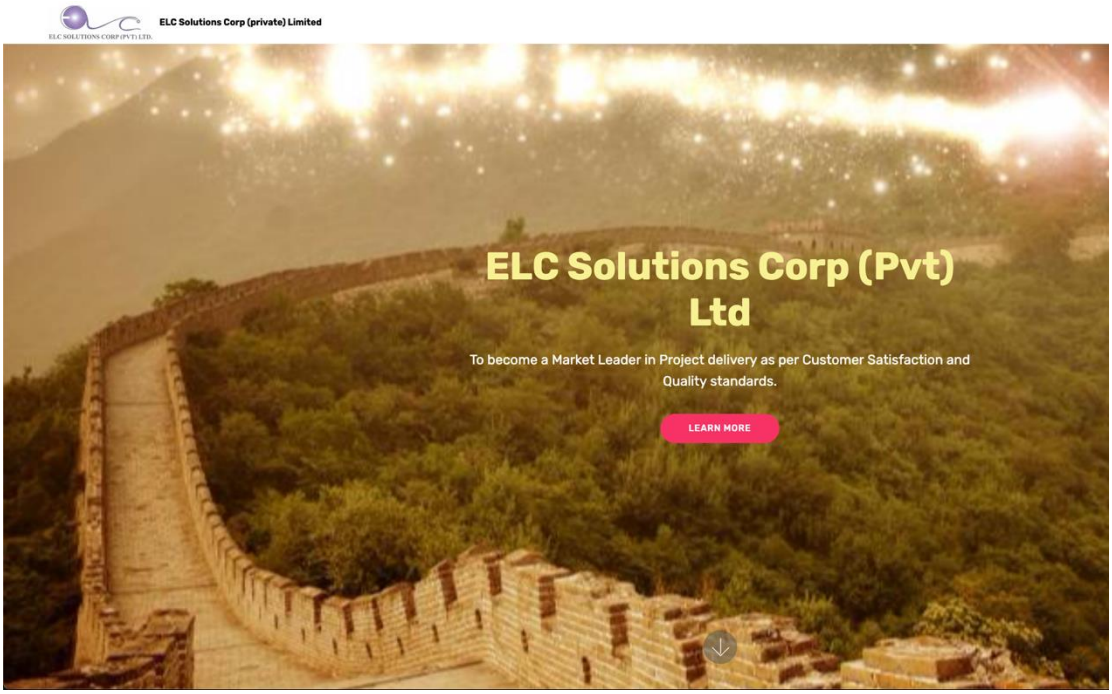


Figure 1 - a screenshot of the ELC Solutions' landing page on their website, showing a picture of the Great Wall of China.

HARDWARE PRODUCTS SHIPPED BY ELINC TIED TO GEEDGE NETWORKS DEPLOYMENT

The trade records show the equipment sent by ELINC to ELC Solutions in September 2023 included computer servers, fibre-optic cabling, network switches and a product termed "UTR PROBE-40" (see Annex 2, 10.1).

While Amnesty International was not able to determine the meaning of UTR, the term "UTR" in "UTR PROBE-40" appears to be a specific reference to the Geedge Network project in Pakistan. The UTR term was consistently used in the Geedge dataset when referring to the Pakistan project, with documents frequently titled either "P19 UTR" or "WMS UTR".

The acronyms P19 and WMS are used interchangeably when referencing to the Geedge Networks work in Pakistan. P19 ("Project 19") is internal codename that was used by Geedge Networks for their Pakistan project. WMS refers to Web Monitoring System, the public facing name for the Pakistani monitoring system.

Separately, further technical records and communications show that representatives of ELINC and Geedge Networks worked closely on deploying the server hardware in Pakistan. The leaked dataset includes records of communications and discussions between ELINC and Geedge related to the correct placement and configuration of servers in two WMS 2.0 data centres, MSH (PTCL Misri Shah) and TWA (Transworld Associates), both located in Karachi, Pakistan.

[227] ELC Solutions, ELC Solutions Corp Achievements, https://www.elccorp.net/Accomplishments.html (accessed on 19 August 2025).

ELINC appears to have be deploy involved in the technical deployment of the systems on-site, with numerous discussions between the two companies on the correct network layout and configuration for the systems. Records from Geedge Networks show that the system was successfully deployed and interception begun. In one communication, Geedge Networks confirmed to ELINC that communication metadata (specifically RADIUS information) from four telecommunications providers was successfully flowing through the WMS 2.0 system in the MSH data centre.

Taken together, the shipment records and leaked communications show that ELINC and Geedge Networks were both intimately involved in the planning and deployment of the Geedge Networks' WMS 2.0 system in Pakistan. These findings also confirm that the network and telecommunications products sent to Pakistan by ELINC to ELC Solutions are highly likely components for the WMS 2.0 interception system.

Further records - documented in the Geedge dataset - of meetings with Pakistani officials, trade data between ELINC and ELC Solutions in Pakistan, and additional OSINT research, allow Amnesty International to concluded with high confidence that Geedge Networks' firewall and interception technologies have been deployed in Pakistan.

4.2 GEEDGE NETWORKS' PRODUCTS

Geedge Networks offers a variety of network management and interception products. This section provides an overview of key Geedge Networks, including but not limited to products that may have been deployed in Pakistan. The product descriptions are based on corporate marketing materials and user documentation included in the Geedge Networks leak.

The following technical analysis is aimed at researchers and practitioners with expertise in network and surveillance technologies. These overviews are important for researchers to assess how firewalls supplied by Geedge Networks work in practice. Section 4.3 then draws on Geedge dataset to present an overview of Geedge Networks' firewalls as they operate in Pakistan.

4.2.1 TIANGOU SECURE GATEWAY

Tiangou Secure Gateway (or TSG) is Geedge Networks' main product, allowing administrators to firewall network streams and enforce network policies, lawful interception and visualization. It is also an operating system that consists of various network components for DPI, interception, man-in-the-middle network connections as well as network injection on HTTP or HTTPS if a root-certificate is installed that can issue certificates, to replace a binary with a malicious binary through a network hijack.

Notably, it has support for Radius traffic to interface with telecommunication networks and apply traffic rules so data can flow through the TSG system. This can be as fine-grained as special traffic rules per subscriber-id found in one of the telecommunications providers. As well as voice over IP (VoIP) records as listed in the administrator guide of the TSG, it can be used to open holes in the firewall where Network Address Translation (NAT) is enabled.

As the system is also able to intercept traffic and store it in a system for later detailed analysis, it is important to see the firewall system also as a surveillance system, where it is possible to enable specific rules for specific users on the network and to keep a log if they commit any network violations, for example using a VPN, Tor network or Psiphon, or try to access censored social media platforms (for example, X in Pakistan). On 7 May 2025, during the armed engagement between Pakistan and India, X became accessible in Pakistan for the first time since February 2024. What drove the decision to unblock X, or who gave the order, has not been disclosed. This lack of transparency has been a feature of previous decisions to block or unblock websites, suggesting that these decisions may be arbitrary.

While WMS 2.0 is able to store data showing which users are using a censorship circumvention tool and which IP addresses visited certain websites, Amnesty International has only been able to find one occasion – through a support ticket that was submitted to Geedge Networks – where two emails with full content and attachments, including the email password, were intercepted. The communications were between a global shipping and logistics company and a Pakistani company involved in tracking of cargo. The number of intercepted emails is likely much higher as the reason why this was intercepted was that no secure connection through TLS was used to authenticate the email platform.

4.2.2 APPSKETCH

AppSketch is a traffic classification system that is available in Geedge Networks' TSG firewalls. It is part of Geedge's DPI product, which determines what application is being used on the network, irrespective of port, protocol, encryption or any "evasive tactic used by the application".[228]

4.2.3 CYBERNARRATOR

CyberNarrator is a product from Geedge Networks that allows automatic classification of traffic and tagging of IP addresses. For example, on the Geedge Networks website it shows a classification of an IP address with "Snowflake", which might be Torproject's Snowflake, a censorship circumvention tool that lets users access websites normally blocked on the censored network.

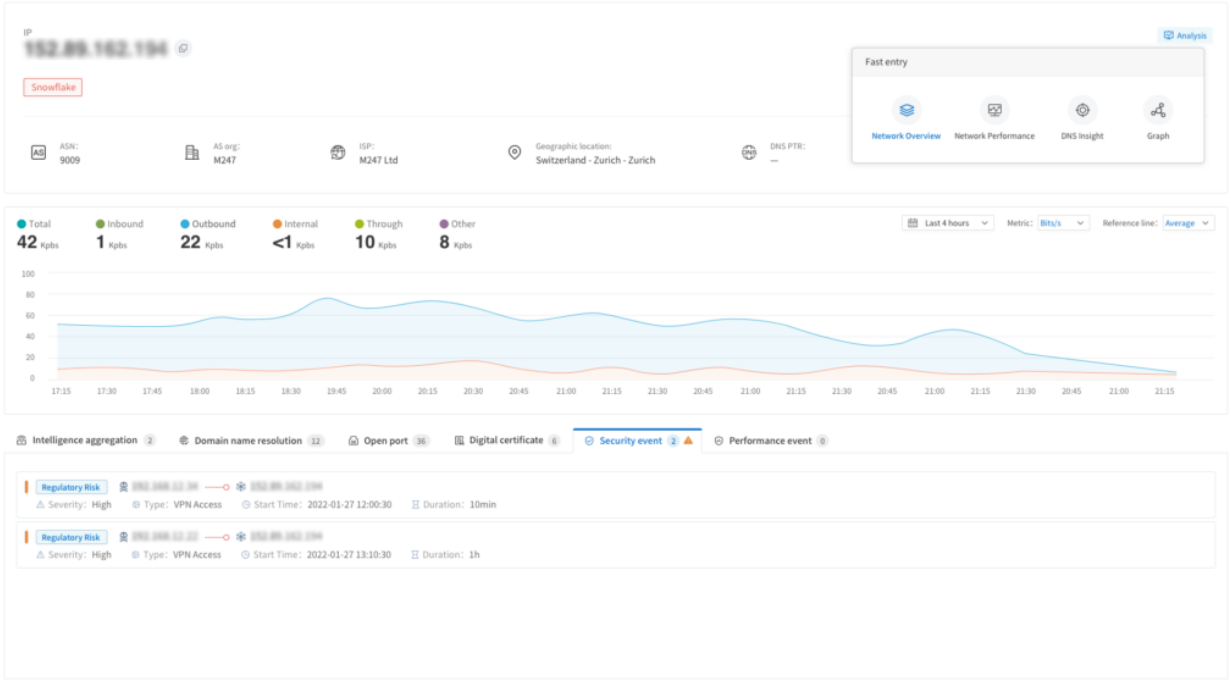


Figure 2 - Screenshot of CyberNarrator obtained from Geedge Networks' website which lists an IP address, provider, location and a tag of "Snowflake". Blurring of images done by Geedge Networks.

4.2.4 NETWORK ZODIAC

Network Zodiac is Geedge Networks' asset inventory system. It allows users to integrate hosts that make up Geedge Networks' system, see deployment details, query logs and statistics of network traffic going over the system, and see where problems might have occurred and if action is required to fix these issues.

4.3 DEPLOYMENT OF GEEDGE NETWORKS' PRODUCTS IN PAKISTAN

One of the most important revelations from the Geedge dataset is how technologies from different suppliers can be interdependent and repurposed to work together. For companies that export sophisticated forms of censorship or surveillance technology or hardware, this demonstrates a critical risk. While an exporter of

[228] Obtained from Geedge dataset: TSG_Administrator's_Guide_Latest_EN.pdf – page 21

such technologies may assess the risks of abuse at the point at which a product is sold, the evidence from Pakistan shows how sophisticated products can be repurposed, and used to harm human right, for many years.

As outlined in 3.3.3 above, WMS 1.0 was first installed in Pakistan in 2019, based on technology provided by Sandvine. Documentation from the Geedge dataset shows how Geedge Networks' technologies have been used to update and advance the WMS.

4.3.1 CODENAME: P19

The Jira contains information on the WMS 2.0 set up by Geedge Networks in Pakistan. The deployment has several code names: P19, WMS-UTR and WMS.

One of the documents mentions a demonstration environment for Pakistan for Geedge Networks' TSG with a licence called "P-Demo" created on 26 June 2023. The demonstration was for two mini-pc's, presumably to show the capability of the system and/or for engineers to experience deploying and testing the system in a lab environment.

On a leaked Geedge Networks' Confluence instance, there is a page for a licence renewal template which mentions the PTA, a date of issuance of 21 September 2023 and date of expiration of 21 October 2023. While the duration of the licence is only one month, we see through a support request in 2024 that the PTA again has access to a licence valid from 11 October 2024 to 1 February 2025.

In the same screenshot we can see what products the PTA has licensed from Geedge Networks:[229]

Product Line: TSG

License Type: Commercial

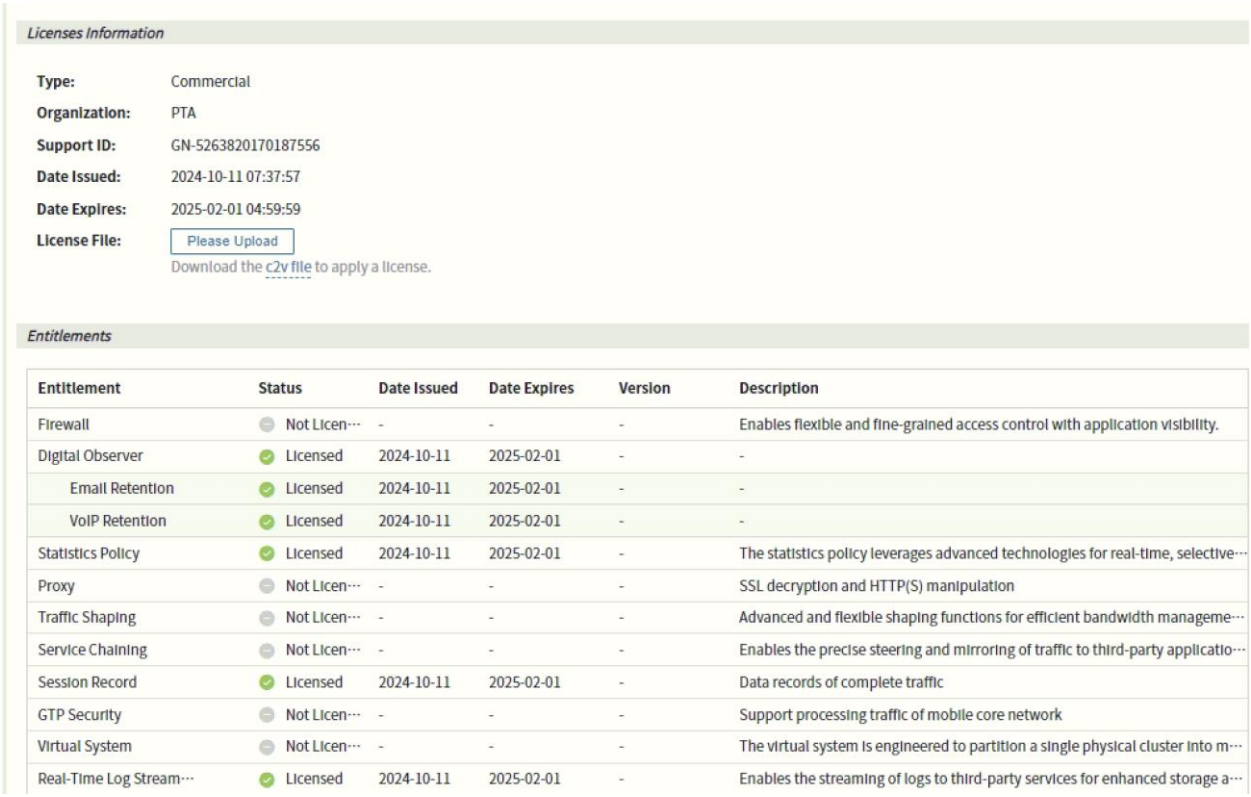
Organization: PTA

Support ID: GN-3124790217244479

Date Issued: 2023-09-21 14:01:33 UTC+5

Date Expires: 2023-10-21 04:59:59 UTC+5

[229] Obtained from Geedge dataset: 邮件模版 License Renewal Notification.html



Licenses Information

Type: Commercial
Organization: PTA
Support ID: GN-5263820170187556
Date Issued: 2024-10-11 07:37:57
Date Expires: 2025-02-01 04:59:59
License File: Please Upload
Download the c2v file to apply a license.

Entitlements

Entitlement	Status	Date Issued	Date Expires	Version	Description
Firewall	Not Licen···	-	-	-	Enables flexible and fine-grained access control with application visibility.
Digital Observer	Licensed	2024-10-11	2025-02-01	-	-
Email Retention	Licensed	2024-10-11	2025-02-01	-	-
VoIP Retention	Licensed	2024-10-11	2025-02-01	-	-
Statistics Policy	Licensed	2024-10-11	2025-02-01	-	The statistics policy leverages advanced technologies for real-time, selective···
Proxy	Not Licen···	-	-	-	SSL decryption and HTTP(S) manipulation
Traffic Shaping	Not Licen···	-	-	-	Advanced and flexible shaping functions for efficient bandwidth manageme···
Service Chaining	Not Licen···	-	-	-	Enables the precise steering and mirroring of traffic to third-party applicatio···
Session Record	Licensed	2024-10-11	2025-02-01	-	Data records of complete traffic
GTP Security	Not Licen···	-	-	-	Support processing traffic of mobile core network
Virtual System	Not Licen···	-	-	-	The virtual system is engineered to partition a single physical cluster into m···
Real-Time Log Stream···	Licensed	2024-10-11	2025-02-01	-	Enables the streaming of logs to third-party services for enhanced storage a···

While the firewall component of Geedge Networks in the above screenshot is not listed as licensed, this part of the PTA licensed Geedge Networks seems to only have software components licensed for retention of e-mail, VoIP, sessions and real-time logs, indicating that the Geedge Networks products might be storing data on who is calling whom, email content if no secure communication is used, session recordings of which websites are being visited and real-time logs of the deployed system.

Another document shows the design of the WMS as of 20 July 2023, operating the TSG platform on repurposed Sandvine hardware from the first iteration of the WMS. The same document also shows Niagara Network fibre splicers being repurposed so the internet traffic from the fibre networks can be mirrored passively or actively and then inserted into the firewall system from Geedge Networks. These machines are produced by Niagara Networks (see 4.5.1, below), presumably using hardware from WMS 1.0 that was procured by Inbox and SN Skies; two companies located in Pakistan. Through trade records, Amnesty International saw that Niagara Networks and Sandvine hardware was delivered to the Pakistani companies Inbox, SN Skies and A Hamson. Similar Sandvine and Niagara Networks equipment show up in an image[230] obtained from the Geedge dataset (see figure below).

[230] Image obtained from the Geedge dataset: 104769585_attachments_image-2023-7-20_15-31-54.png

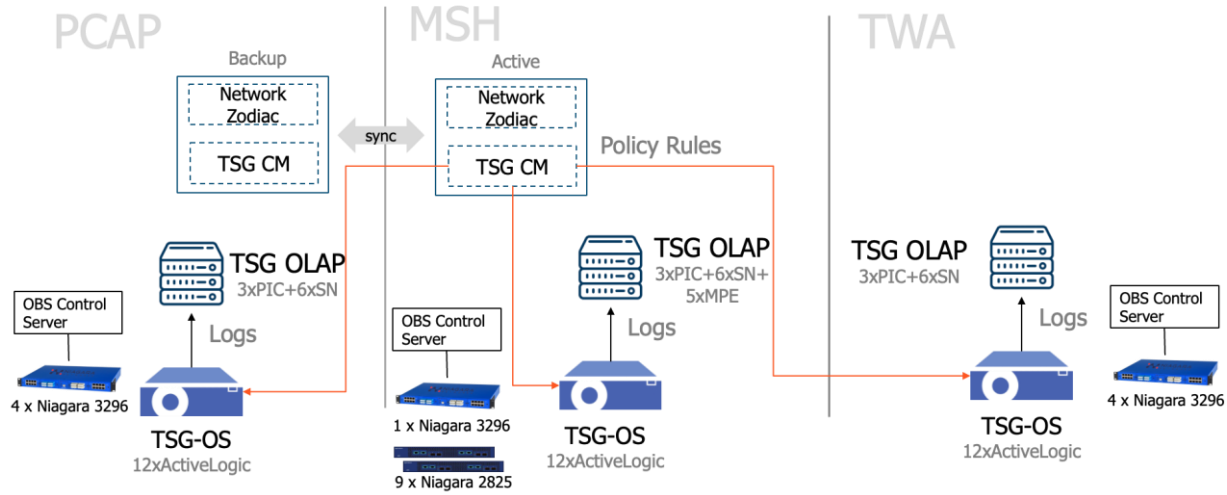


Figure 3 - Extracted image from Geedge dataset showing repurposed Sandvine and Niagara Networks equipment for an early setup with Geedge Networks software.

The document further explains how Geedge Networks' TSG-OS is installed on Sandvine's hardware in Pakistan for WMS 2.0. It is installed at two different sites: MSH (Misri Shah) and TWA (Transworld Associates). Both are network locations where the Geedge Networks system is deployed.

TWA refers to the infrastructure provided by Transworld Associates (Pvt.) Limited (Transworld), a telecommunications provider in Pakistan that makes internet access possible through fibre-optic cables laid down in the ocean between Oman and Karachi. TWA is also mentioned in the tender from the PTA where the WMS is installed at the fibre-optic Hawks Bay Landing Station, where one of the internet cables that provides connectivity comes onshore in Pakistan. PCAP, a data centre in Pakistan, is likely the site where internet traffic flowing through the cables is intercepted and stored. While full content capture seems unlikely due to the sheer amount of traffic flowing through the cables, it seems more likely that certain internet session metadata is being stored. These parsed fields of an email containing content and metadata seems to be confirmed by looking at the binaries and the SQL tables that are set up for the TSG Galaxy product, which is the analytical database utilized by Cyber Narrator (see section 4.2.3) to store its DPI data. The SQL data reveals a substantial amount of internet session data is being stored this way, including the full content of emails when no encrypted connection such as STARTTLS or SSL/TLS is possible.

From the dataset, Amnesty International was able to obtain an example of the TSG Galaxy product being leveraged in Pakistan. A support ticket (in Jira) from WMS 2.0 sent to Geedge Networks' support function seems to list the metadata and full content of two emails, including the subject, protocol, attachment names, who is being emailed, the sender and the IPs involved. As the intercept was attached to a support ticket, Amnesty International was able to verify that one of the email servers of the sender did not support a secure encrypted connection, and the functionality to intercept unencrypted email is enabled in Pakistan because of Geedge Networks' products. Therefore, anyone who connects to an email server that does not support secure encrypted connections, such as TLS, risks the interception of email content in Pakistan.

The support tickets[231] also seem to indicate that the repurposed Sandvine devices have been set up by A Hamson. Running the firewall is not without issues. The dataset consisting of support tickets include the packet loss during peak hours on smokeping[232] results from Pakistan Telecommunication Company Ltd (PTCL). On 28 July 2023 and 1 August 2023, A Hamson opened a ticket (GTS-7) detailing that some websites were not being blocked adequately, trouble with the Niagara Networks devices and the bypass on 15 September 2023. The bypass happens when traffic is prevented from reaching the WMS 2.0 TSG servers or, in simpler terms, it cannot drop the traffic from reaching a blocked website and therefore the blocked website can be accessed by internet users.

In a Confluence document detailing WMS 2.0 and its status on 8 December 2023, the presence of the WMS is indicated in several points:

[231] Obtained from the Geedge dataset: GTN-507 WMS Issue Analysis.html
[232] Smokeping is a way to measure, store and display latency in the observed network.

- IGW Karachi (Zong)
    - 5.2Tbps
    - Also known as the “VOIP Command Center”
- PTCL Pak Capital Telephone Exchange
    - 24x100GE
    - 1.8Tbps
- PTCL Misri shah (MSH) Telephone Exchange
    - 24x100GE
    - 1.8Tbps
- Transworld Associates Cable Landing Station
    - 24x100GE
    - 1.6Tbps
    - Total URL Current entries 650,000

These cable landing and exchange locations seem to largely overlap with WMS 1.0.

In a later set up, as documented on WMS 2.0 on 22 May 2024, it is indicated that the WMS is now implemented at three international exchanges in Karachi with a combined 5.2Tbps of network traffic. It is mainly processing unencrypted traffic (10% of the traffic) such as HTTP or SIP, also known as VoIP from the MSH data centre.

A diagram in the same leaked Confluence document shows how a lawful intercept system, presumably the LIMS system, is relying on data that has already gone through the WMS system (for a more detailed analysis of LIMS, see 5.2.1.)

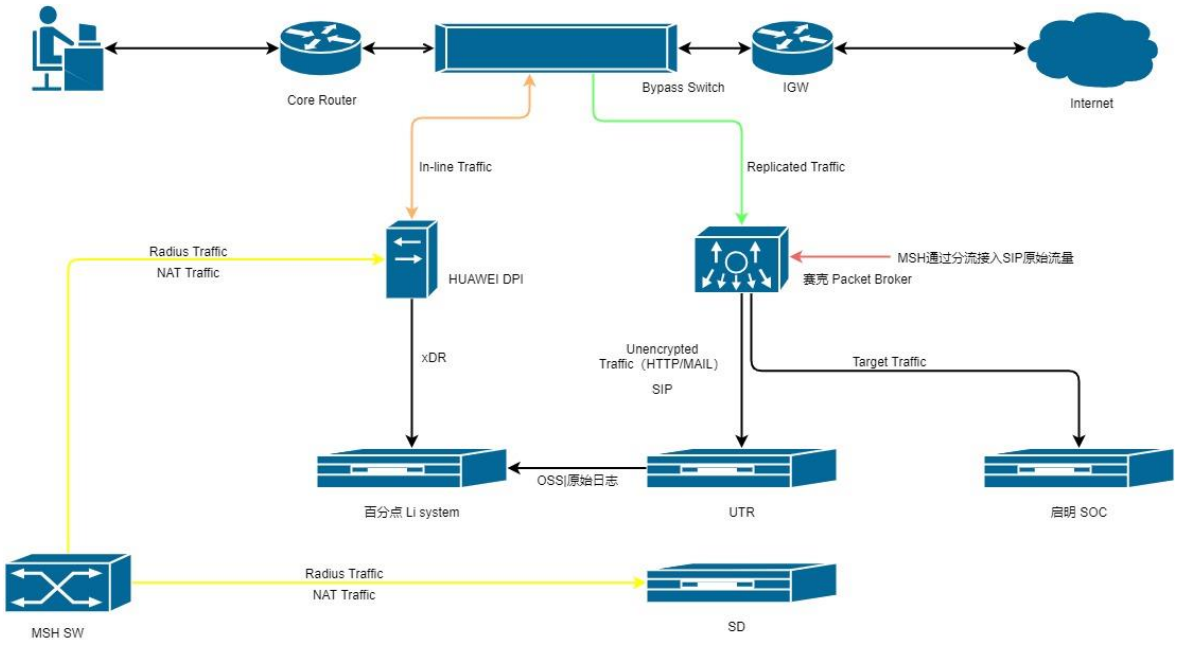


Figure 4: A map of how the various components of the WMS system integrate, and which data centres are available for what specific amount of traffic.

Unencrypted data passing through the WMS system seems to be saved for future analysis by those who may have access to the Geedge’ system and that would include the PTA. The diagram also includes a label listing “Huawei DPI”. Amnesty International does not have any further information on the Huawei DPI system

named in this diagram. In August 2025, Amnesty International wrote to Huawei to ask if it had supplied any DPI technology to Geedge Networks or to any other entity in Pakistan. Huawei did not reply by the time of publication.

We do know the lawful intercept system is run by Datafusion, with the LIMS software from Utimaco.

The TSG system by Geedge Networks is able to interface with several telecoms providers through RADIUS, which allows the Geedge system to access billing data and the ability to route mobile internet traffic through the WMS:

- China Mobile Pakistan Limited (CMPaK Limited), trade name Zong.
- Pak Telecommunication Mobile Limited, trade name Ufone.
- Pakistan Mobile Communications Limited, trade name Jazz.
- Telenor Pakistan (Pvt.) Limited (Telenor).

An Excel spreadsheet obtained from the Geedge dataset contains all the NAT device IPs and IPV4 and IPV6 segments, as well as how to map individual users on the basis of NAT device-IP and its corresponding radius device-IP in the case of Jazz.

Several screenshots reviewed by Amnesty International also show problems with the WMS system interfacing to Zong and Jazz RADIUS backends and IP addresses.

4.4 HOW GEEDGE NETWORKS' TECHNOLOGY ENABLES CENSORSHIP IN PAKISTAN

Government-installed firewalls as a system of censorship may take many forms. To block free access to the internet, firewalls can restrict certain websites or content online. When governments do this, they are restricting various human rights including the rights to freedom of expression and access to information, freedom of association, freedom of peaceful assembly, health and education, among others. The human rights impacts of disruptions may be especially pronounced for women, children, LGBTI people and marginalized communities.

The locations for the internet gateways are listed in the tender document as:

1. PTCL IGE-I, Pak Capital Exchange, Karachi.
2. PTCL IGE-II, Marston Exchange, Karachi.
3. PTCL IGE-III, Satellite Town Exchange, Rawalpindi.
4. PTCL Misri Shah Exchange, Karachi.
5. TWA, Hawks Bay Landing Station, Karachi.

The total volume of internet traffic passing through these internet gateway sites at the time was 1.5 Tbps.

Through the Geedge dataset and the Open Observatory for Network Interference (OONI) explorer, Amnesty International identified categories of online content, websites and applications that are blocked in Pakistan.

4.4.1 WMS BLOCK LISTS CATEGORIES

While the information in the Geedge dataset does not show contracts or non-disclosure agreements with companies in Pakistan, there are documents and diagrams detailing the demonstration environments of the WMS, the telecommunications providers connected to the WMS, the network problems due to broken memory modules for the hardware, and the fact that the PTA is the authority adding websites to the block list.

Amnesty International did not identify which websites or VPN providers are on the block list, but the block categories include VPNs and certain protocols such as QUIC, websites with sexual content ("PTA-Blocking-PornWebsites"), "Immoral/indecent" and "Anti state category". These last two categories in particular show how dissent and expression are being censored within Pakistan.

The block list categories listed are:

- PTA-Blocking-PornWebsites
- PTA-PornWebsite-ServerIP
- PTA-category-blocking-HTTP
- PTA-blocking-HTTP
    - Escorts, Malicious, MOI-MOI
    - CSAM
    - Anti state category
    - Immoral/indecent
    - PTA-1 Pornography
    - PTA-2
    - PTA-4
- PTA-blocking-QUIC
- Monitor_VPN_Customer_Outbound
- Monitor_VPN_Customer_Inbound
- Test_Monitor_Outbound
- Testing_monitor_IP
- PTA_MONITOR_TESTING_IP
- PTA_TEST_IP_MONITOR
- SHOQ_MON_IP
- PTA-URL
- URL_Keywords
- BLOCK_URLs

In addition to a block list, the WMS has an "allow list". Amnesty International did not identify which websites are on the allow list but could infer applications or websites based on the name of the allow list.

Allow list:

- TWA_WHITELIST_POOL_POLICY_Dst
- JAZZ_TAMSHA_SHUNTED_LIST
- TWA_WHITELIST_POOL
- Whitelist_Policy_ONIC

The allow list features telecommunications providers including ONIC from PTML, Tamsha on Jazz (Tamsha might be short for tamasha, a video-on-demand platform and connectivity provider), and Transworld Associates (listed as TWA). Meaning that there's special allow lists for certain kinds of traffic and from certain providers, although it remains unclear what those allow lists contain.

4.4.2 NETWORK BLOCKADES OBSERVED BY OONI

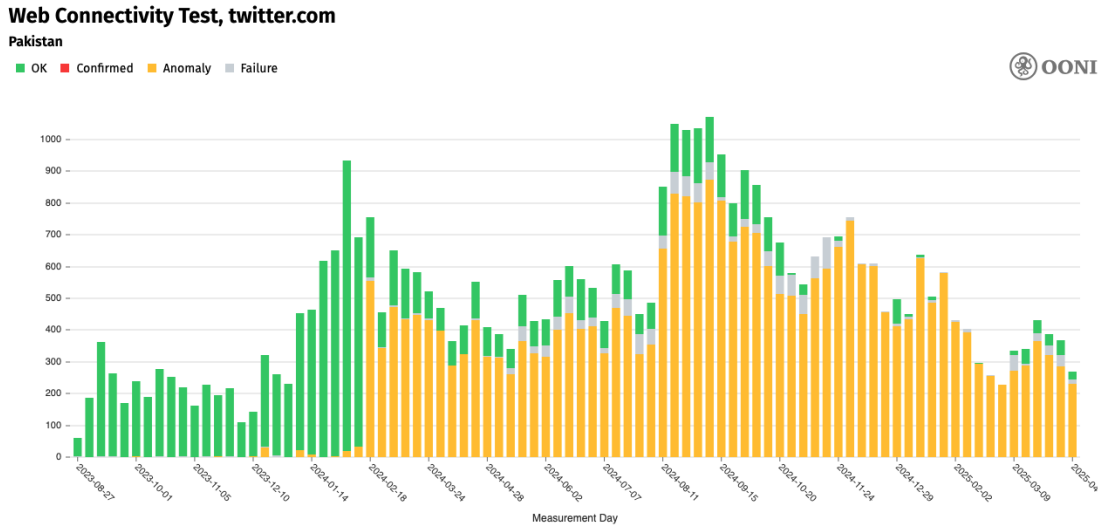


Figure 5: A map of how the various components of the WMS system integrate, and which data centres are available for what specific amount of traffic.

OONI makes software that relies on crowdsourced measurements collected through apps or their website, with that information being reported back to the OONI team. Some of these tests rely on scanning whether a large list of websites, technology and apps are reachable and working on networks as they should be. If that is not the case, anomalies are shown on the OONI Explorer.

After consulting the OONI Explorer and its analysis of some block attempts, some applications and websites can be seen as blocked within the firewall of Pakistan. One notable example is the social media website X, which was blocked between 17 February 2024 and 7 May 2025,[233] as well as the messaging applications Telegram and Signal.

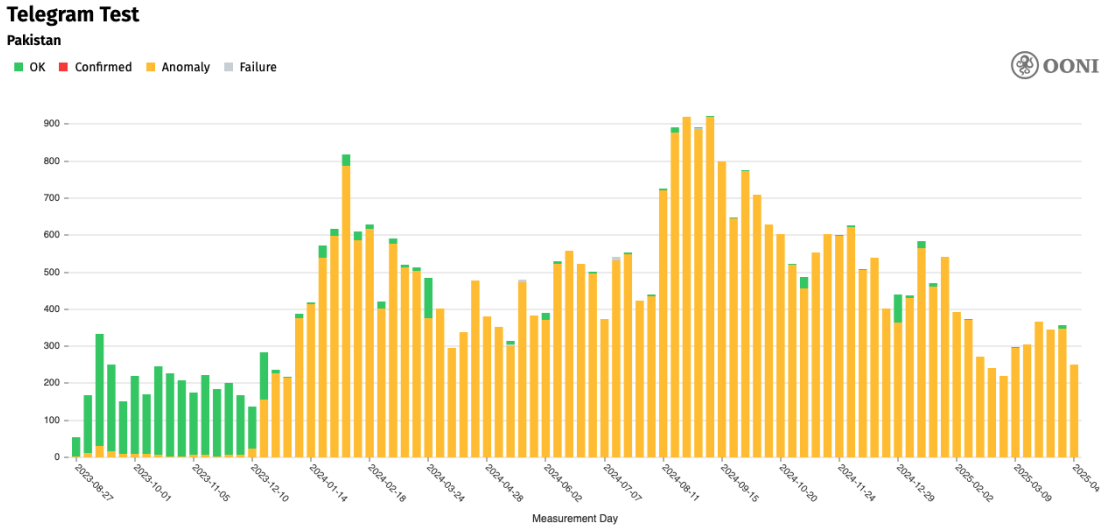


Figure 6 - Shows OONI results and a high amount of anomalies when accessing the Telegram service.

[233] OONI, OONI Measurement Aggregation Toolkit (MAT), https://explorer.ooni.org/chart/mat?probe_cc=PK&test_name=web_connectivity&domain=twitter.com&since=2025-04-18&until=2025-07-18&axis_x=measurement_start_day&time_grain=day (accessed on 19 August 2025).

Telegram appears to have been blocked on or around 16 December 2023, according to the analysis by OONI, and the block can be seen in the graph above as ongoing at the time of writing.[234]

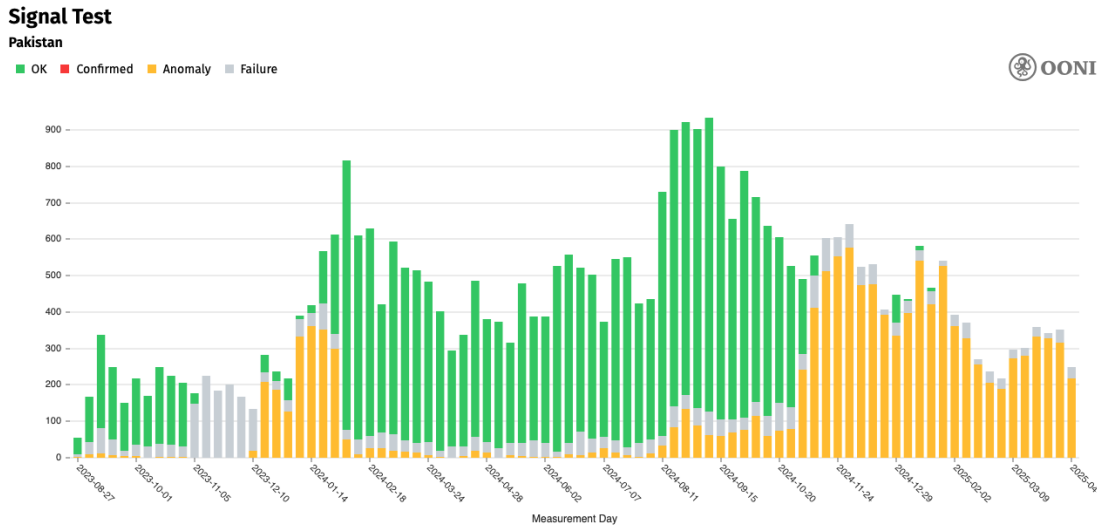


Figure 7 - Shows OONI results with a high amount of anomalies for accessing the Signal infrastructure.

Secure messaging application Signal also seems to have had issues. Network anomalies can be observed from December 2023 to January 2024, when it was unblocked. New network anomalies can be observed starting around October or November 2024 and were ongoing at the time of writing.

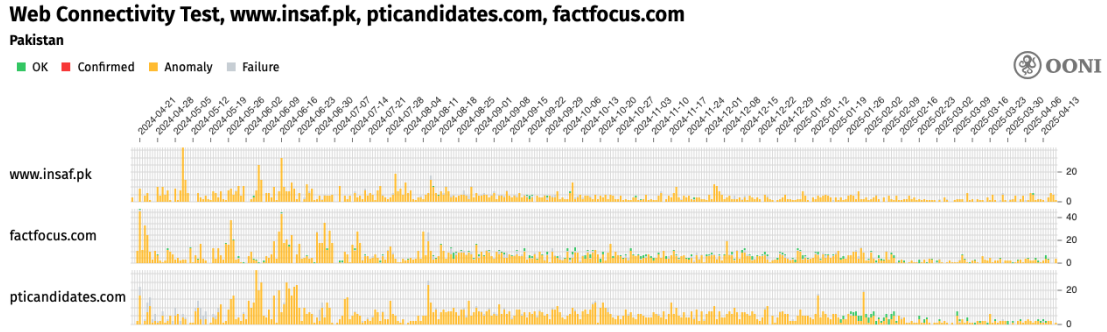


Figure 8 - Shows OONI results and a high amount of anomalies for attempting to access websites, www.insaf.pk, pticandidates.com and factfocus.com.

Just before the general election on 8 February 2024, OONI measurements confirm that several websites were blocked, including the opposition PTI party website and the PTI candidates' website, as well as Fact Focus, an investigative news outlet. The founder[235] of Fact Focus is currently under investigation for allegedly sharing content criticizing the armed forces.[236] This shows that the new firewall, as deployed by Geedge Networks, is being used effectively by Pakistani telecommunications providers to actively block crucial communication channels, including social media platform X, as well as an opposition party website and an investigative news outlets.

[234] OONI, Pakistan blocked Telegram, https://explorer.ooni.org/findings/324516225200 (accessed on 19 August 2025). (accessed on 25 August 2025)
[235] His two brothers were forcibly disappeared in March 2025.
[236] Voicepk, "FIA books journalist Ahmad Noorani in train attack 'propaganda", 15 March 2025, https://voicepk.net/2025/03/fia-books-journalist-ahmad-noorani-in-train-attack-propaganda (accessed on 25 August 2025)

Amnesty International was unable to conclude whether the WMS was able to differentiate between lawful and unlawful traffic. An employee of an telecommunications provider shared that "the current monitoring and blocking systems in place cannot differentiate between legitimate and non-legitimate traffic."[237]

4.5 COMPANIES ENABLING THE WMS

This chapter has outlined the operations of WMS 1.0 (primarily based on Sandvine hardware) and WMS 2.0 (primarily based on Geedge Network hardware). As Amnesty International researched the implementation of the WMS, several other companies emerged as playing key roles in its installation and operations.

4.5.1 NIAGARA NETWORKS

Screenshots obtained by Amnesty International through the Geedge dataset show that Geedge Networks made bespoke software to interface with Niagara Networks devices that make passive and active tapping possible. In the deployment in Pakistan, Niagara Networks devices were used in both WMS 1.0 and WMS 2.0. This hardware was acquired through private companies: shipping records obtained by Amnesty International show that Niagara Networks has shipped hardware to SN Skies and Inbox Business Technology in Pakistan. The dataset further reveals that A Hamson worked with Niagara Networks devices that are running at telecommunications providers.

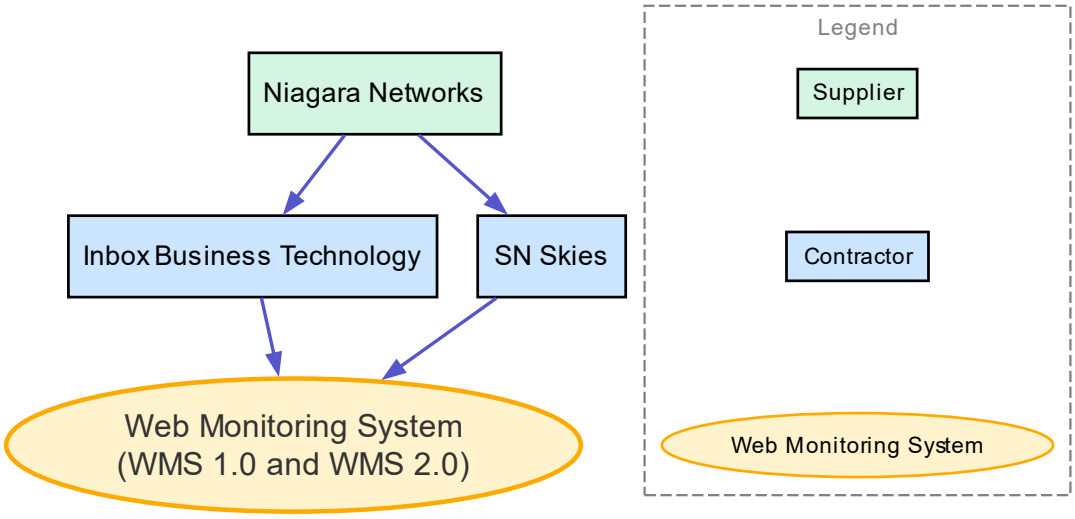


Figure 9 - Shows an image with Niagara Networks as a supplier to Inbox Business Technology and SN Skies as contractors for the WMS 1.0 and 2.0.

The usage of Niagara Networks devices is not limited to Pakistan. In the dataset there are other occurrences of the use of the devices in other countries where Geedge Networks has customers.

[237] Cite interview

```
root@passivetap-1:/home/pta/TWA/TAP-1# ./geedge_tool -get -info
Device Serial Number [1F30O0C0122210017 ]
Init Serial [1F30O0C0122210017 ]

N3296 Device Status:

Relay status
-------------------------------------------------------------------------
| segm 1 | segm 2 | segm 3 | segm 4 | segm 5 | segm 6 | segm 7 | segm 8 |
-------------------------------------------------------------------------
| bypass | bypass | bypass | bypass | bypass | bypass | bypass | bypass |
-------------------------------------------------------------------------
```

Figure 10 - this image shows a computer terminal interface, presumably logged in to an Niagara Networks device, where it requests the N3296 status worth the fibre bypass. The /home/pta/ indicates the user as the PTA and TWA as the Transworld Associates location. This image was obtained from the Geedge dataset.

In the figure above, a Niagara Networks N3296 device is being operated. It shows a commandline programme called "geedge_tool" that reads the device serial number and shows which ports are in what network mode. In this case, they are all in bypass mode. It seems that the user on this N3296 is "pta", which likely refers to the PTA in Pakistan. TWA likely refers to a location from TWA where the device is in use.

Amnesty International is aware of trade data, obtained from subscription-based trade platforms, that show that Inbox Business Technology received Niagara Networks' 3296 devices. Additionally, trade records show that Niagara Networks in the United Arab Emirates (UAE) delivered a "2847 main chassis, ac. S2 versi" to SN Skies. Versi is likely to be the abbreviation of "version". This Niagara Networks 2847 device is a hardware component that can be used for analysing traffic from multiple fibre-optic cables and traffic streams redirected into WMS. It allows the user to combine multiple connection streams to be put into another device for further monitoring and/or analysis.

4.5.2 COMPANIES ENABLING WMS 1.0

Section 3.3.3 outlined the installation of the first iteration of the WMS, using Sandvine technology, referred to in this report as WMS 1.0. While the use of Sandvine technology for WMS 1.0 has been previously reported on, Amnesty International can reveal two more companies it associates with maintenance of WMS 1.0: SN Skies Pvt Ltd (SN Skies) and A Hamson. Both are located in Pakistan.

SN Skies has corporate presence in Pakistan, the UAE, USA, UK and Afghanistan. The company reveals on its website that it has partnered with the Pakistani government to build a government data centre, and that it has deployed a "Web Management System", an alternative name for the WMS, at the SCO-IGW site, a likely international gateway operated by the Special Communications Organization, operated by the Ministry of Information Technology and Telecommunications, for "200G of international traffic using advanced DPI and machine learning analytics".[238] SN Skies also lists a project for which it deployed a URL and application filtering solution at Transworld (TWA). Transworld's infrastructure is listed in the tender document published by the PTA as one of the international internet gateway data centres at which it plans to deploy a WMS system. Amnesty International was not able to confirm whether the filtering solution was part of the WMS.

[238] SN Skies, https://snskies.com/ (accessed on 10 August 2025).

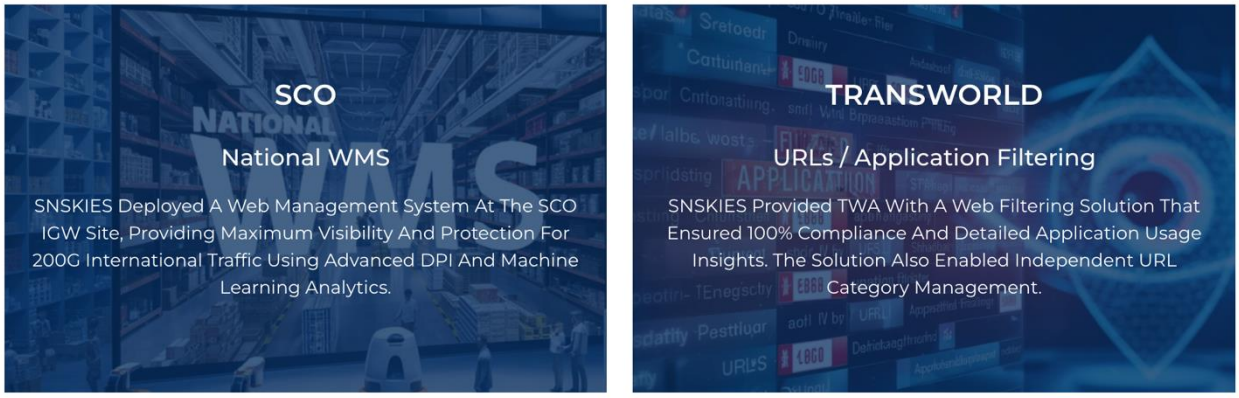


Figure 11 – Screenshot of two projects on which SN Skies has worked, involving the WMS at the SCO internet gateway as well as an URL and application filtering solution at the internet provider and internet gateway of Transworld.

A Hamson, SN Skies and Inbox Business have all received Sandvine hardware, as revealed through trade data.

DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE
21 JUNE 2017	Sandvine Inc	Sn Skies Pvt Ltd	42 units	NETWORKING EQUIPMENT	N/A
5 JULY 2019	Sandvine Inc	A Hamson Pvt Ltd	32 units	SANDVINE NETWORKS	N/A

Table 1- Table of trade data showing Sandvine Inc shipping SN Skies a total of 74 units of equipment. Once on 21 June 2017 and 5 July 2019. There's no declared value.

For Inbox Business Technology trade data, see Annex 2, 10.11: "Inbox Business Technologies Pvt. Ltd."

This trade data reveals that A Hamson received Sandvine equipment from Sandvine in Canada in 2019. It is therefore possible that this equipment has been used in WMS 2.0 (see Section 4.3.1).

A Hamson has a corporate presence in Pakistan, the UAE, Canada and the UK.

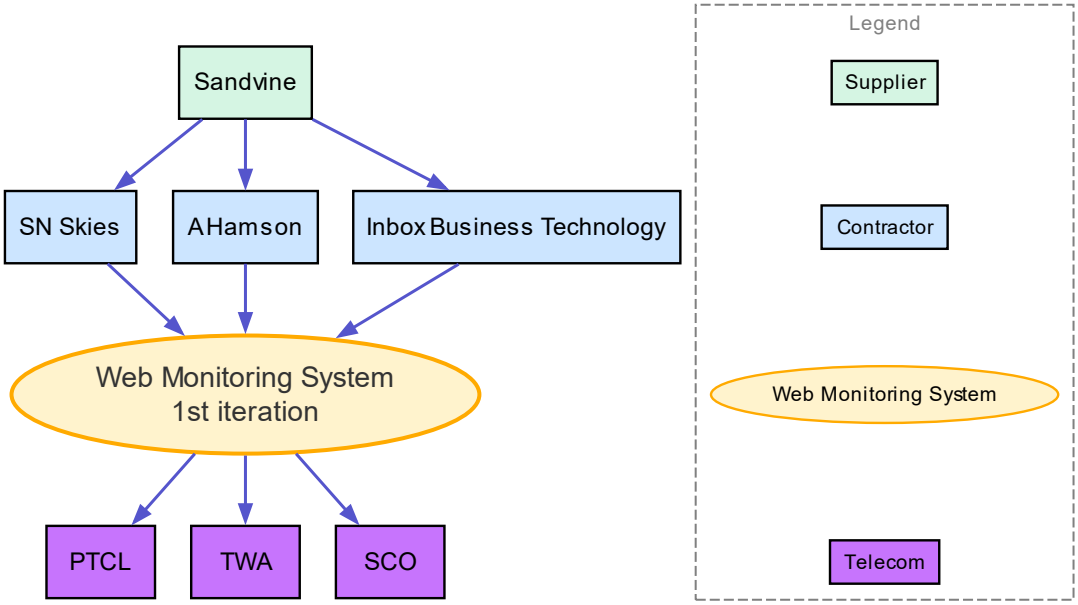


Figure 12 - shows Sandvine was a supplier to SN Skies, A Hamson and Inbox Business Technology for WMS 1.0 that was installed at PTCL, TWA and SCO.

4.5.3 COMPANIES ENABLING WMS 2.0

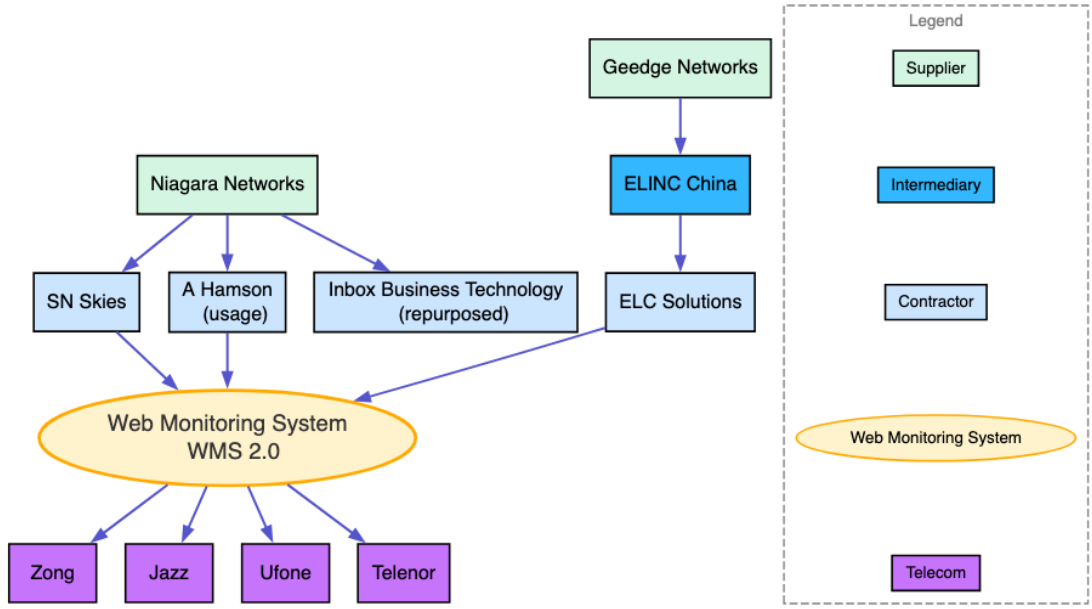


Figure13 shows Niagara Networks shipping equipment to SN Skies and Inbox Business Technology to be used at the WMS 2.0. A Hamson uses this equipment to make the WMS 2.0 possible. Additionally, Geedge Networks, through ELINC China onwards to ELC Solutions shipped

THALES DIS (FORMERLY GEMALTO)

Thales DIS is owned by the French defence giant Thales S.A., trading as Thales Group, which makes a variety of products that allow interfacing with hardware tokens and software licensing, among other products. As customers of Geedge Networks procure a licence, that licence is only valid for a certain amount of time before the system will stop functioning. This specific licensing software used by Geedge Networks is made by Thales DIS (formerly Gemalto). In the Geedge dataset Amnesty International reviewed licensing screenshots, both Gemalto (now Thales DIS) are displayed, indicating a longer history between Geedge Networks and Thales.

The software in question is called Sentinel, described as a software licensing security solution on Thales' website.[239] Geedge Networks' product relies on licences that are installed by Geedge Networks employees into the setup and, without a valid licence, the firewall would stop working. The Sentinel licensing software is thus an integral part of the Geedge Networks product, as deployed in Pakistan, and is provided by Thales.

[239] Thales, Digital Identity and Security, https://www.thalesgroup.com/en/markets/digital-identity-and-security (accessed on 12 August 2025).

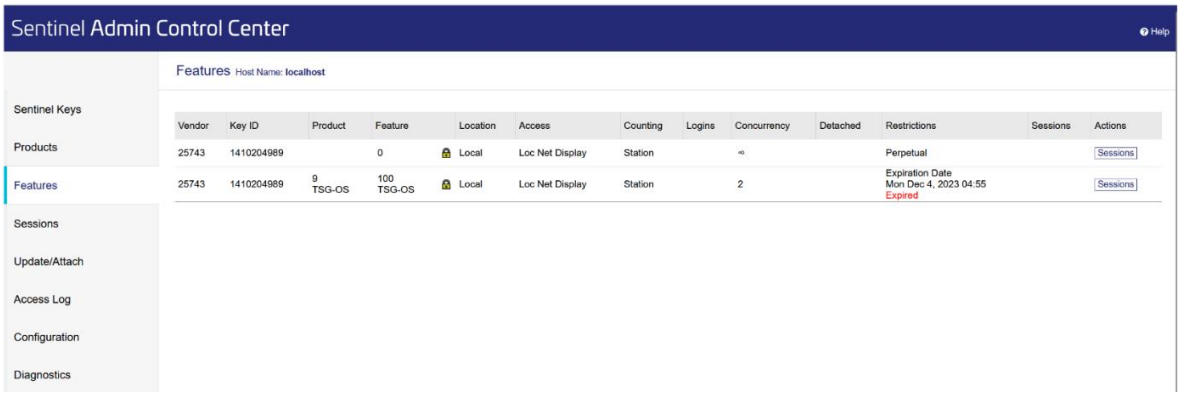


Figure 14 – Screenshot of Thales' Sentinel Admin Control Centre, mentioning one of the products – TSG-OS – which is licensed to one of Geedge Networks' customers.

NEW H3C TECHNOLOGIES

Chinese-based company New H3C Semiconductor Technologies Co., Ltd (H3C) is a server provider for Geedge Networks and was used in the WMS 2.0 installation setup by Geedge Networks, as identified through screenshots in the Geedge dataset.

Please refer to Annex 2: Commercial trade data records for trade data that Amnesty International obtained from subscription based trade platforms, notably from ELC Solutions Corp (Pvt) Ltd to find shipment of H3C equipment.

Figure 15 – Extracted screenshot from the Geedge dataset showing the MSH deployment in Pakistan making use of H3C R4900 servers.

The commandline interface of a Linux system shows root@msh-h3cr4900-olap001. H3C R4900 is a server series by New H3C Semiconductor Technologies Co., Ltd.[240] The servers and other hardware were delivered by ELINC to a Pakistani company in November 2023, indicating that H3C servers ended up serving the WMS 2.0. In January 2025 a second hardware delivery was made to ELC Solutions (see Annex 2, 10.1).

[240] New H3C Semiconductor Technologies Co., Ltd. was added on the United States entity list by the Bureau of Industry and Security, Commerce on 26 November 2021. Federal Register, Addition of Entities and Revision of Entries on the Entity List; and Addition of Entity to the Military End-User (MEU) List, 26 November 2021, https://www.federalregister.gov/documents/2021/11/26/2021-25808/addition-of-entities-and-revision-of-entries-on-the-entity-list-and-addition-of-entity-to-the (accessed on 25 August 2025)

5. COMPANIES ENABLING MASS SURVEILLANCE IN PAKISTAN

Mass surveillance by the Pakistani authorities is predominantly managed through LIMS. The LIMS system allows DPI that can detect a wide range of internet data, allowing for the interception of targets' communications when they are entered into the LIMS system.

While section 3.2.2 provides background on the purpose and legal basis for the use of the LIMS system, as well as the ways in which this system violates human rights in practice, this chapter focuses on the companies that supply the technology to enable LIMS to operate – German-based Utimaco and UAE-based Datafusion – and their products. Utimaco and Datafusion have delivered their technologies to Pakistani telecommunications providers, enabling indiscriminate interception of the population's communications. This section shows how international companies have continued to supply increasingly sophisticated mass surveillance technologies to Pakistan, despite mounting evidence of their potential for misuse. Amnesty International spoke with people working at telecommunications providers who claimed to know little to nothing about the monitoring centres within their organizations. This indicates that information is tightly controlled around the monitoring centers installed at the telecommunications providers, even to those who should be in the know about this.[241]

5.1 THE RELATIONSHIP BETWEEN UTIMACO AND DATAFUSION

Datafusion Systems (Datafusion) has been active in the interception of telecommunication and also the voice biometric market for more than three decades.[242] Some of Datafusion's products rely on technology from other vendors. Datafusion has partnered for more than a decade with Utimaco, a company headquartered in Germany. While operating independently of each other, Datafusion relies heavily on Utimaco's lawful-intercept technology in its products. Utimaco lists both Datafusion and Trovicor (Datafusion's former name) as partners on its website.[243] Utimaco also produces security technologies including encryption software and hardware. This report only looks at its lawful-intercept technology product, LIMS.

Datafusion has traded under different names and been located in various countries around the world. Datafusion has a corporate presence in countries including Czechia, Germany, the UAE, Malaysia and Pakistan. While Datafusion has previously had its corporate headquarters in Germany and then Malaysia, it is currently located in Dubai, UAE. In a 2017 YouTube video, its then managing director stated that reasons for moving Datafusion's development from Germany to Malaysia included cost as well as rumours of new

[241] Amnesty International is not naming the individuals in order to protect their security.
[242] Datafusion Systems https://datafusion.ai/ (accessed on 18 August 2025).
[243] Utimaco, Utimaco Partners: Datafusion, https://utimaco.com/partners/datafusion (accessed on 18 August 2025): Utimaco, Utimaco Partners: Trovicor, https://utimaco.com/partners/trovicor (accessed on 18 August 2025).

stricter EU export regulation.[244] In 2023, Datafusion was acquired by Boss Industries SAS., located in France. On 3 July 2025, Lumine Group, based in Canada, announced at it had completed its purchase of Datafusion.[245]

While Datafusion's customer list is not publicly available, a video on its website featuring one of the company's previous managing directors discusses its products and "active 35 installations around the world", as well as a world map with red dots indicating where active installations are located.[246] One such location seems to indicate Pakistan. Others include customers in other Asian countries, the MENA region, Africa, Europe and the USA or Canada.

↑ *Figure 16 - video still from a Datafusion video from 2017 showing where its clients are located.*

Additionally, Datafusion claims in its ethics committee report that it follows human rights standards from the UN and the Organisation for Economic Co-operation and Development (OECD), among others. According to Datafusion's annual report to its ethics committee in 2021, "Datafusion's human rights assessments are robust and meaningful, and the company routinely declines business opportunities that would present unacceptable risk".[247]

Datafusion in its annual report has also stated that it used an internationally recognized human rights expert to review potential sales opportunities in 2022, but it is not clear who this person was. The company has failed to publish any updates from its ethics committee since 2021. Such lack of transparency raises questions about Datafusion's commitment to ensuring human rights standards are met when their products are exported, as well as whether and how they track how their products are used.

EU companies exporting powerful dual-use surveillance technologies can escape EU regulatory frameworks by operating in other jurisdictions where regulations are less stringent. The ability of companies to engage in jurisdiction-shopping within the EU and to utilize corporate structures available in jurisdictions which are more lax on export control has long been a cause for concern for Amnesty International.[248]

---

[244] YouTube, Malaysia Digital Economy Corporation, Panel discussion: "Cybersecurity Investment Footprint in Malaysia", 16 August 2021, https://youtu.be/MjLpmM93OFc?t=372

[245] Lumine, "Lumine Group Completes the Purchase of Datafusion Systems", 3 July 2025, https://www.luminegroup.com/newsroom/lumine-group-completes-the-purchase-of-datafusion-systems/ (accessed on 25 August 2025)

[246] YouTube, "trovicor/datafusion interview", 10 October 2024, https://youtu.be/bI5GDSKL7sQ?t=213

[247] Trovicor, *Annual report of the Ethical Committee 2021,* https://web.archive.org/web/20220820131653/https://trovicor.com/wp-content/uploads/ethical-committee-report-2022.pdf (accessed on 25 August 2025)

[248] Amnesty International has highlighted this issue in, *The Predator Files; Caught in the net,* October 2023, https://www.amnesty.org/en/documents/act10/7245/2023/en/ For a broader discussion of EU regulation of surveillance technology exports, see *Out of Control: Failing EU Laws for Digital Surveillance Export.* September 2020, https://www.amnesty.org/en/documents/eur01/2556/2020/en/

In Utimaco's case, it is unclear how the company conducts human rights due diligence in selecting business partners, such as Datafusion, or when it would stop a partnership due to human rights concerns.

Utimaco's LIMS product is export-controlled in the EU and Germany. This means that Utimaco must request an export permit from the German government in order to export it. Datafusion appears to have exported LIMS technology through its UAE entity to several Pakistani telecoms providers, according to information obtained by Amnesty International from subscription-based trade platforms. It is unclear whether Utimaco or Datafusion requested export permits from the UAE authorities for a re-export, or if this was part of the original permit.

5.2 UTIMACO PRODUCTS

5.2.1 LIMS

LIMS is a DPI solution built by Utimaco that allows traffic from telecoms providers to be identified, intercepted and queried by law enforcement officials. Amnesty International was able to obtain a brochure uploaded to the website slideshare showing the lawful interception capabilities of LIMS and found that it can intercept different GSM protocols such as 2G, 3G, 4G and 5G as well as DSL, VOIP, VoLTE and others.[249]

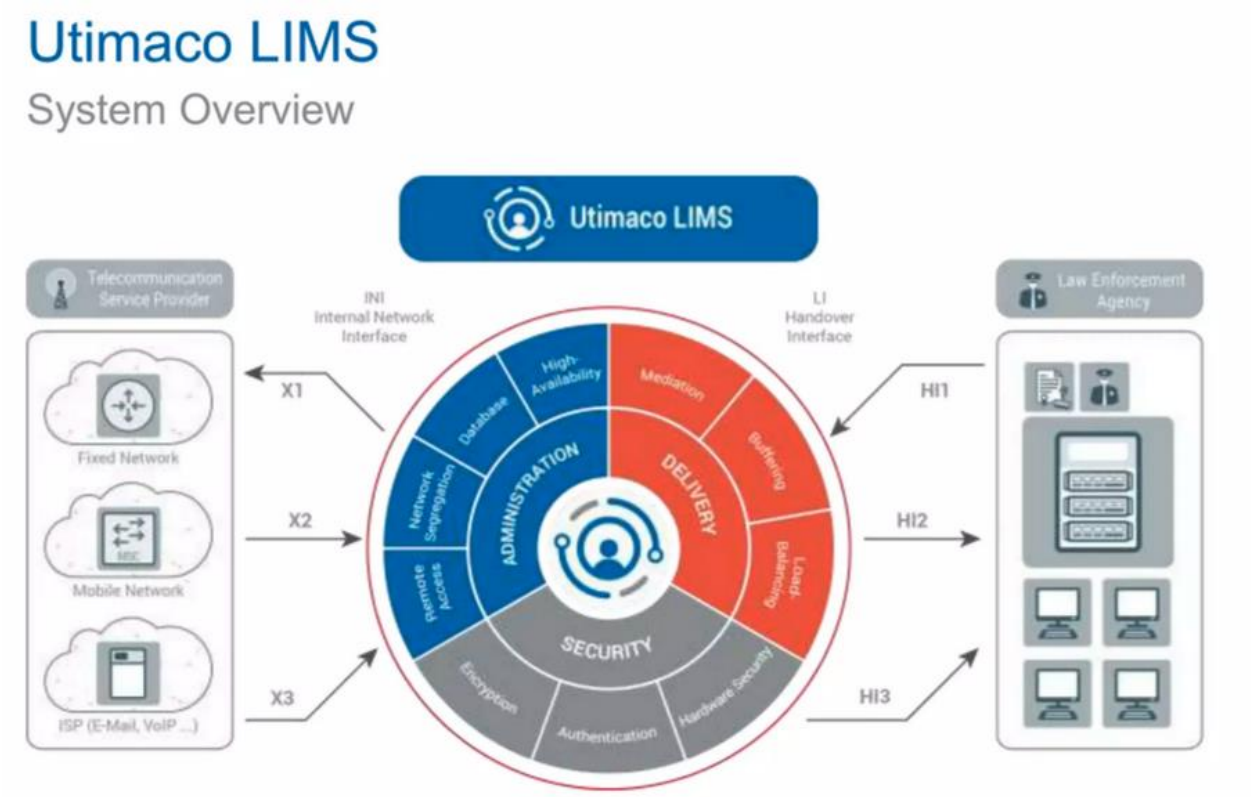


Figure 17 – Utimaco brochure showing how data is passed from telecommunications providers through the LIMS software, so law enforcement can search through the wiretapped data.

[249] Slideshare, LI Solutions, June 2018, https://www.slideshare.net/denyszb/li-solutions (accessed on 25 August 2025)

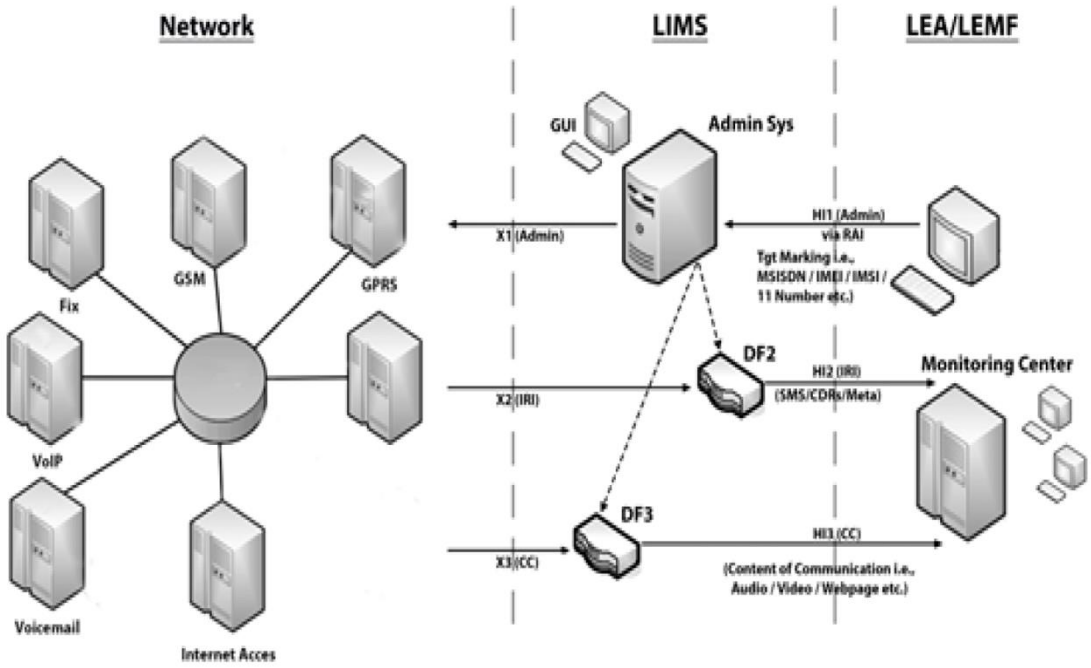


Figure 18 - Chart illustrating LIMS as presented to the IHC (2024).

An older Utimaco LIMS brochure from the early 2010s, published by Wikileaks, shows that it provides central administration of intercepts and a way to add targets for interceptions. The key features as described in the brochure are "active and passive interception of voice and data services" as well as delivery of the intercepted communications to the appropriate law enforcement agency.[250]

5.3 DATAFUSION PRODUCTS

Datafusion sells various surveillance technologies and methods to connect different data sources together and mine them for patterns. Little is known about how customers deploy the system and use the data retained.

Nevertheless, some light can be shed on the products' capabilities from descriptions on the various websites that Datafusion has maintained throughout the years, as well as sales brochures obtained from trade shows which Datafusion attended.

5.3.1 MONITORING CENTRE NEXT GENERATION

Datafusion's Monitoring Centre Next Generation (MCNG) allows operators to query intercepted data from telecoms providers and other data sources, analyse the data, and exploit it for speaker identification, gender and language detection as well as keyword spotting and session correlation on encrypted over-the-top voice&video, e.g, to figure out who is calling whom using Signal that's normally encrypted and legacy technologies like PTSN calls and faxes.

[250] WikiLeaks, Spy Files: *Ultimaco LIMS Lawful Interception of Telecommunication Services,* 15 September 2014, https://wikileaks.org/spyfiles/docs/UTIMACO-LIMSLawfInte-en.pdf (accessed on 25 August 2025)

5.3.2 TACTICAL SOLUTIONS

While Datafusion's website has scarce information on its "tactical solutions" product line, a trade brochure obtained by Amnesty International shows that products advertised in the past by Amesys and Nexa Technologies continue to be sold under the company name of Datafusion. Amnesty International previously wrote about the "alpha-max" interception system when investigating the Intellexa alliance in 2023.[251] The Intellexa alliance is no longer active, although the company Intellexa is.

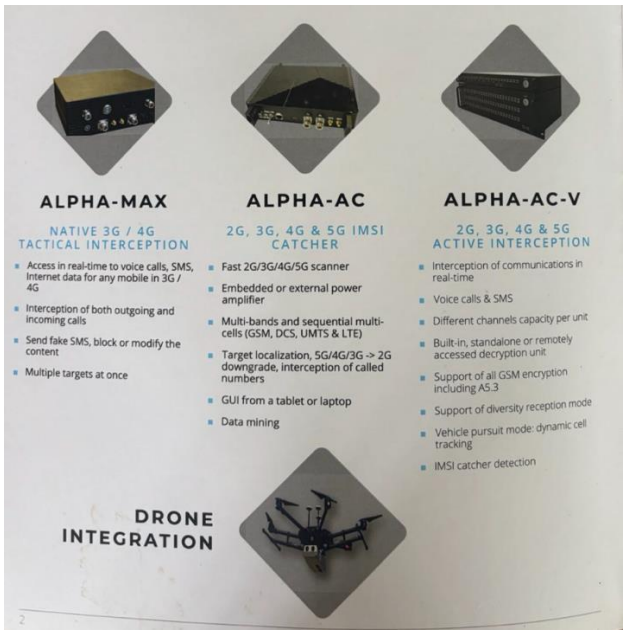


Figure 19 - Datafusion is showcasing their Alpha devices which is an interception technology for GSM communication and a way to integrate those into a drone.

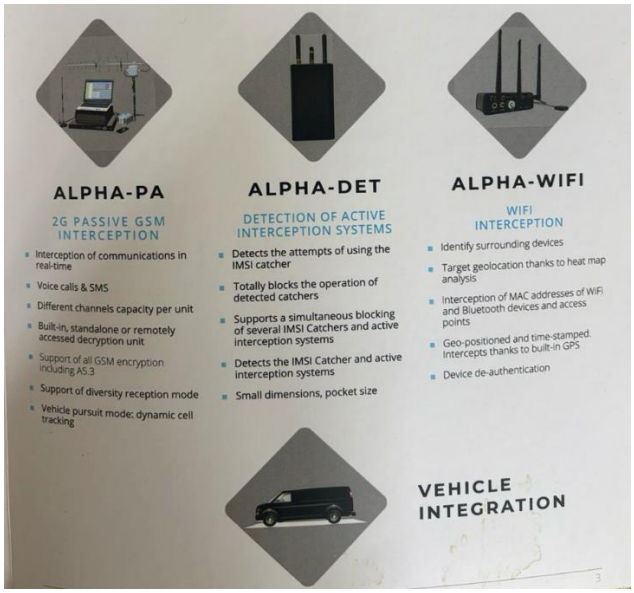


Figure 20 - More Alpha devices which can be used to intercept GSM traffic with, as well as a separate device to intercept WiFi communication and a way to integrate these Alpha devices into a vehicle.

[251] Amnesty International, Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products, 6 October 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/

Public posts on social media provide further insight into how Datafusion products operate. Posts on X by a now former Datafusion employee and who worked from the Datafusion Malaysian subsidiary, describe how certain customers deploy the products:

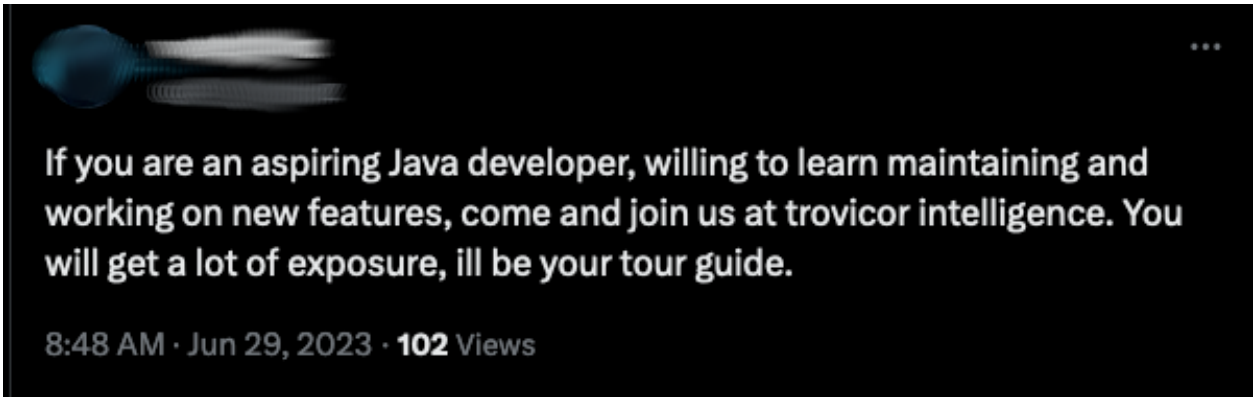


Figure 21- A now former employee of Datafusion posted saying: "If you are an aspiring Java developer, willing to learn maintaining and working on new features, come and join us at trovicor intelligence. You will get a lot of exposure, I'll be your tour guide."

Another post by the same account on X mentions an unknown customer allegedly located in the Middle East and mentions the use of LTO storage tapes[252] on which to store data.

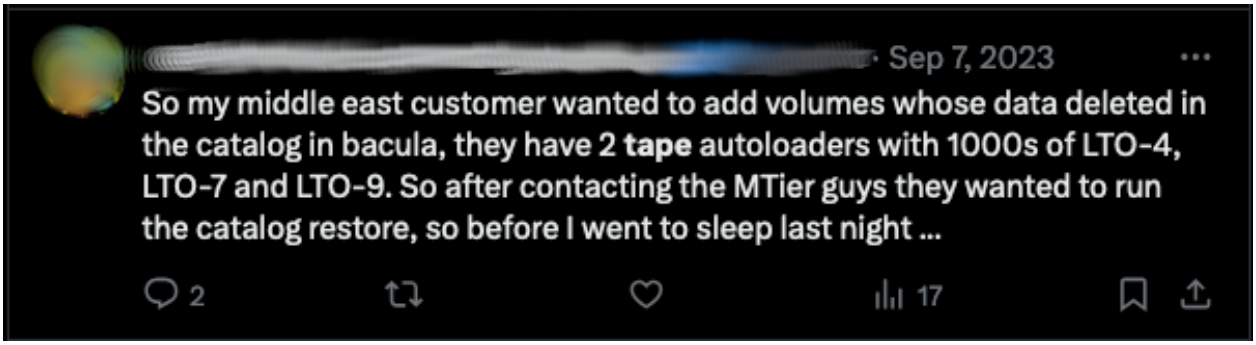


Figure 22 - The same employee posts on X about a customer in the Middle East who is storing data on thousands of LTO storage tapes.

Another post explains that the deployed systems are airgapped, or not connected to any network to be administrated remotely, and information is stored on tapes. A single LTO-9 tape can store up to 45 Terabytes of information or the approximate equivalent of around 9 million mp3 songs, enough to play music continuously for approximately 1,000 years. The deployed systems and storage tapes are likely used to store intercepted information or metadata for the customers data retention system.

The social media posts on X are unfortunately no longer available.

5.4 DATAFUSION AND UTIMACO IN PAKISTAN

Amnesty International's research indicates that Datafusion and Ultimaco's tools have been used in Pakistan for many years. A 2015 research report by Privacy International looked into surveillance products used by

[252] LTO storage tapes are tapes, similar to a cassette that allows to write data on.

law enforcement in Pakistan, and showed Utimaco and Datafusion providing interception capabilities to the telecommunications providers Ufone, Telenor and Jazz, among others.[253]

Amnesty International obtained commercial trade data showing shipments to Pakistani customers of Datafusion between 2014 and 2024. These shipments comprised computer hardware such as routers and switches to allow interfacing with network equipment from telecommunications providers, among others.

Some of the trade data contains descriptions such as "SERVERS MCNG STORAGE SERVER", "RACK MOUNT FIBRE BYPASS SWITCH 3808C NIAGERA NETWORKS" and "LIMS MEDIATION DEVICE FOR ZTE LIG UP TO 400,000 SUBSCRIBERS SOFTWARE". This kind of equipment makes it possible for anyone who has access to Datafusion's monitoring centres deployed at telecommunications providers to intercept, store and analyse data, as well as query the data. "LIMS" refers to the product provided by Utimaco.

As the trade data shows, Datafusion provided a 3808C fibre bypass switch from Niagara Networks to Cyber Internet Services (trade name Cybernet), such that Niagara Networks' hardware is used in both LIMS and in the WMS 2.0 system.

Amnesty International has trade data revealing records of software, hardware and LIMS shipments being made to several telecoms providers in Pakistan including Zong, Jazz, Telenor, Warid Telecom (now acquired by Jazz) and Cybernet, a business-to-business telecoms company that also provides a submarine internet communication cable that connects Pakistan to Egypt and France through the PEACE cable.[254] Combined, the telecoms providers mentioned have 85% of the telecommunication market share in Pakistan.[255]

The trade data shows that Datafusion has also sold MCNG equipment to Zong, Ufone and Telenor. Such sophisticated monitoring centres can surveil and sift through the content of an individual's texts and phone calls and location. (See Annex 2: Commercial trade data records.)

Amnesty International looked for mentions of Utimaco and Trovicor/Datafusion from former employees on Linkedin and found evidence that someone allegedly working for Datafusion in Karachi had experience of integrating Utimaco products.

[253] Privacy International, *Tipping the scales: Security & surveillance in Pakistan*, July 2015, https://privacyinternational.org/sites/default/files/2018-08/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf (accessed on 25 August 2025)
[254] Cybernet, "Cybernet and PEACE complete construction from Pakistan to France", 29 September 2022, https://cyber.net.pk/peace-completes-construction-from-pakistan-to-france/ (accessed on 25 August 2025)
[255] Pakistan Telecommunication Authority, market share, https://web.archive.org/web/20250523153530/https://www.pta.gov.pk/category/telecom-indicators/166 (accessed on 21 August 2025)

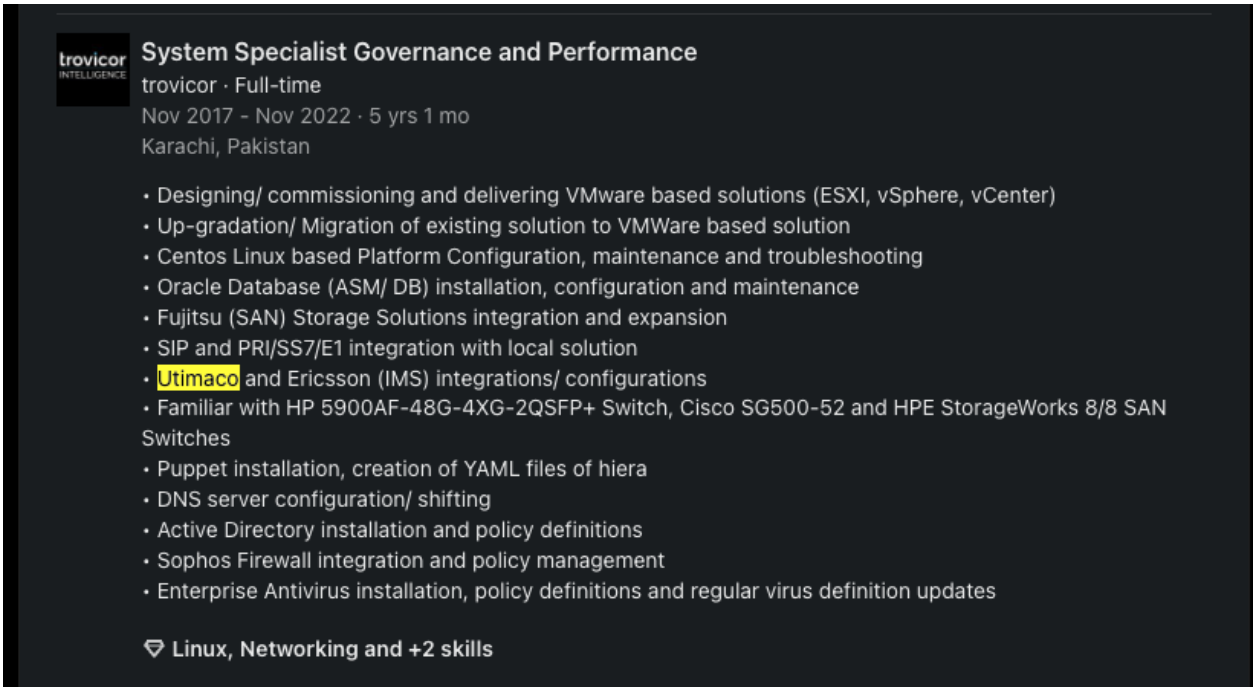


Figure 23 - An alleged former employee shared on their LinkeDin profile that they were a former Trovicor employee based in Pakistan who has experience working with Utimaco configurations.

6. COMPANIES' LINKS TO HUMAN RIGHTS VIOLATIONS IN PAKISTAN

Amnesty International has documented numerous human rights abuses related to the use of surveillance and censorship technologies by governments around the world, based on an analysis of state obligations under international human rights law[256]. While the Pakistani authorities are primarily responsible for the human rights violations caused by their mass surveillance and unlawful internet censorship, this report sheds light on the previously obscure role of private companies in supplying the technology used by the authorities in doing so. This report has outlined how a broad range of surveillance and censorship technologies have been exported to, and deployed in, Pakistan. These technologies are being used as part of a system of mass surveillance by the Pakistani government, including allowing warrantless access by ISI to the phone records of Pakistani citizens; and to enable internet censorship that has included frequent internet shutdowns.

As laid out in the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), companies have a responsibility to respect human rights in their operations, products and services. A company may exacerbate or facilitate human rights abuses through, among other things, the provision of goods and services. The UN Guiding Principles outline that companies have a responsibility both to ensure that they do not cause or contribute to human rights abuses across any of their business activities, and to respond to human rights abuses when they occur, and to provide remedy when appropriate. The UN Guiding Principles also call for companies that are directly linked to a human rights abuse through their business relationships to use their leverage to prevent the abuse.

Amnesty International has written to the PTA, the ISI and the Ministry of Information Technology and Telecommunications to ask for more information on how it has deployed the surveillance and censorship technologies documented in this report. The Pakistani authorities had not replied at the time of publication, and without access to the technical logs, Amnesty International does not have the necessary information to link the use of any of the specific technologies detailed in this report to specific incidents of surveillance or censorship. Unlike spyware, which may leave a digital trace on the targeted device that may be attributable to a specify company, a mass surveillance system such as LIMS leaves no such trace. Similarly, while this report can outline the technical capacity of the WMS to restrict access to the internet and enable internet shutdowns, it is not possible to determine the cause of any given internet blockage.

However, the UN Guiding Principles outline the responsibility of companies to undertake human rights due diligence based on identifying, preventing, mitigating and accounting for the impact that the business has or may have on human rights, using a risk-based approach.

In the case of Pakistan, the human rights risks associated with the provision of surveillance and censorship technologies to the government should have been abundantly clear to these companies, based on many years of public reporting on the use of surveillance and censorship in Pakistan.

[256] See for example: Amnesty International, The Predator Files: Caught in the Net (Index: ACT 10/7245/2023), 9 October 2023, https://www.amnesty.org/en/documents/act10/7245/2023/en/

Surveillance technologies have been deployed in Pakistan over many years to target dissent, political opponents, human rights defenders and journalists. Internet shutdowns have been used at critical times to block access to information. In addition to widespread reporting of surveillance and censorship abuses such as with LIMS and the WMS in Pakistan, the risks associated with sales to the country are clearly signalled in Pakistan's score on global comparison ratings that are frequently used by companies as part of human rights due diligence policies.[257] Therefore, while the WMS and LIMS cannot be attributed to specific instances, these human rights impacts are necessarily facilitated by these technologies.

In addition to the evidence of misuse of surveillance and censorship technologies, a human rights due diligence process on sales to Pakistan would also be expected to pick up on the lack of safeguards to prevent their misuse. Section 3.3.3 outlines the export of Sandvine's technologies to Pakistan from 2016 to 2022. In 2024, Sandvine announced that it would no longer sell to "non-democratic countries or where the threat to digital rights is too high". One of those countries was Pakistan. However, stopping sales to Pakistan did not remove Sandvine's responsibilities for any human rights abuses committed in the period of its operations, and did not prevent the Sandvine hardware supplied for WMS 1.0 being repurposed in the WMS 2.0 setup by Geedge Networks. Sandvine's actions also raise the question of why, with access to the same information on human rights violations in Pakistan, other companies selling products with comparable risks have continued to sell their products to Pakistan.

In line with the UN Guiding Principles, companies should responsibly disengage from a business relationship or activity where the risks of human rights abuse cannot be adequately prevented or mitigated[258], or these efforts have failed. Given the abundant evidence of human rights risks related to the sale of surveillance and censorship technologies to Pakistan, Amnesty International believes that the companies documented in this report as exporting these technologies to Pakistan – namely, Geedge Networks, Utimaco, Datafusion and Niagara Networks – have contributed to these human rights abuses. As such, and under the UN Guiding Principles, these companies have a responsibility to review their human rights due diligence processes. These companies should also use all leverage to prevent adverse impacts of their operations. Should they be unable or unwilling to do so or should this leverage fail to prevent or mitigate such harms, then these companies should halt all exports to Pakistan until it is clear that sufficient safeguards are in place in Pakistan to prevent their use in human rights abuses.

In addition to the responsibilities that apply to all companies under the UN Guiding Principles, companies may also be bound by specific regulations based on the countries from which they are exporting their products. Surveillance technologies specifically may be classified as dual-use items, meaning that they have both civilian and military applications. Amnesty International and numerous other civil society organizations have long argued that the opacity in the trade of surveillance technologies is fuelling a digital surveillance crisis. The changing and opaque corporate structures of many of these companies, which in some cases have entities in multiple countries, makes it extremely challenging to track the trade in these productsAmnesty International wrote to entities of these companies based on publicly available information contained in various corporate registries or their websites. Amnesty International asked the entities for information about their human rights due diligence practices.

6.1 HUMAN RIGHTS RESPONSIBILITIES OF UTIMACO

LIMS is a DPI solution built by Utimaco which allows traffic from telecoms providers to be identified and intercepted by law enforcement officials (see section 5.2.1). In October 2024, Amnesty International wrote to Utimaco, asking the company to outline any measures it carries out to ensure that its technology is not linked to any human rights abuses, and to share its human rights due diligence policies, as well as any grievance or whistleblowing policies.

Amnesty International also asked Utimaco to clarify its relationship with Datafusion, which exported the LIMS product to Pakistani customers (see section 5.4). Utimaco declined to answer these questions but replied to state that: "We are contractually prohibited from providing information on the specifics of our business partnerships or implementations. In everything we do, we fully comply with the relevant applicable legal

[257] A robust human rights due diligence policy should draw on detailed, specific information on human rights in a country. However, global rankings are frequently used. On both the Freedom House as well as the Economist Democracy Index rating, Pakistan has been sliding down ever since it published the rating in 2017 compared to the rating of 2025. As well as the Freedom on the Net publication by Freedom House that showed Pakistan being classified as "not free" from 2012.

[258] United Nations, Guiding Principles on Business and Human Rights, page 21, section commentary, paragraph 3: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed 21 August 2025)

requirements and export control laws and regulations." Utimaco's full reply to a research letter Amnesty International sent in October 2024 is included in Annex 3.

Additionally, there is no grievance procedure available to the general public or whistleblowers at Utimaco to report misuse of the LIMS product. Utimaco was asked about allegations that it was selling its technology to authoritarian regimes in 2013.[259] The company responded that it followed both German and European export guidelines and restrictions such as the UN sanctions list, and that it audits its systems extensively. However, it is unclear whether Utimaco has ever cancelled contracts with state entities in countries where it has established abuse or where external parties have established abuse.

The German government answered questions from a German MEP on 3 December 2024 relating to the provision of export licences to Datafusion and Utimaco in Germany. However, it stated: "The German government is not providing information on the number of export licences granted to individual companies in order to protect trade and business secrets".[260]

Utimaco is based in Germany and is therefore recommended to follow the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, which provide a framework for companies dealing in surveillance technologies to consider the implications of the export and deployment of these technologies in different contexts and their impact on human rights. Germany is also a signatory to the Wassenaar Arrangement, a voluntary export regime designed to promote transparency in the sale and export of arms and dual-use items.[261] Dual-use items, such as surveillance technologies, can pose specific risks due to their potential use for internal repression or severe human rights abuses. The EU's duel-use export controls were revised in 2021 and stipulate that EU member states should "consider" the risk of human rights abuses, and include enhanced export controls on non-listed surveillance technologies that pose a threat to human rights.[262] According to Utimaco's Export Compliant Policy,[263] both LIMS hardware and software are regulated under Category 5 of the EU's Dual-Use Regulation, which covers telecommunications and "information security".[264] Human rights implications of authorizing an export licence should still be considered by the licensing state; in this case Germany. Amnesty International asked Utimaco what licences it sought for the sale of LIMS to Pakistan. Utimaco declined to answer, citing confidentiality but stating that it complies fully with export control laws and regulations.

As a Germany-based company, Utimaco's LIMS product is export controlled by the EU and Germany. When Utimaco wants to export LIMS, it must request an export permit from the German government. Datafusion (which has corporate entities in both the UAE and Germany) has exported LIMS through its UAE entity (see Annex 2: Commercial trade data records), to several Pakistani telecommunications providers. It is unclear whether Utimaco or Datafusion requested export permits from the UAE authorities for a re-export or if this was part of the original permit given by Germany. When a dual-use item passes through a third country, which then re-exports it, that country must be named in the original export permit.

Amnesty International has not been able to determine what export licences were sought or received for Utimaco to export LIMS, because both Utimaco and the German government have refused to publish or answer questions about these. Utimaco did not reply to Amnesty International's questions about its human rights due diligence policies. Utimaco does not have a clear, publicly available grievance or whistleblowing policy and does not provide any information on cases where it has declined, suspended or modified the use of its products because of the risk of its technology being linked to human rights abuses. Given the extensive, publicly available information on surveillance abuses in Pakistan, as well as previous allegations of Utimaco's links to human rights abuses, Utimaco has not demonstrated that it has been able or willing to conduct adequate due diligence – including by exercising leverage - to ensure that its products are not linked to such human rights abuses, Amnesty International believes that Utimaco should halt all exports to

[259] Business & Human Rights Resource Centre, "Utimaco's response re allegations about its surveillance technology's use by authoritarian governments to target human rights defenders", 20 September 2013, https://media.business-humanrights.org/media/documents/utimaco-re-surveillance-20-09-2013.pdf

[260] Deutscher Bundestag, *Schriftliche Fragen mit den in der Woche vom 2. Dezember 2024 eingegangenen Antworten der Bundesregierung [Written questions with responses from the Federal Government received in the week of 2 December 2024]* (Drucksache 20/14088), 6 December 2024, https://dserver.bundestag.de/btd/20/140/2014088.pdf, p. 8, para. (in German). (accessed on 25 August 2025)

[261] Wassenaar Arrangement Secretariat, *Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (WA-DOC (19) PUB 007), December 2019, https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf (accessed on 25 August 2025)

[262] European Union, Regulation (EU) 2021/821 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, 9 September 2021, https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html (accessed on 25 August 2025)

[263] Utimaco Export Compliance Policy, November 2018, https://utimaco.com/sites/default/files/inline-files/Utimaco_Export_Compliance_Policy.pdf (accessed on 25 August 2025)

[264] European Union Dual-Use Regulation 2021/821, May 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821#d1e32-449-1 (accessed on 25 August 2025)

Pakistan until it is clear that sufficient safeguards are in place in Pakistan to prevent their use in human rights abuses.

6.2 HUMAN RIGHTS RESPONSIBILITIES OF DATAFUSION

Utimaco's LIMS products have been exported to Pakistan by Datafusion (see 5.2.1 and Annex 2). Formerly known as Trovicor and headquartered in Germany, Datafusion is now based in the UAE. In October 2024, Amnesty International wrote to Datafusion, asking whether it had exported LIMS to Pakistan. Datafusion replied on 21 October 2024 declining to answer specific questions, citing strict confidentiality agreements, although it states that its products "are sold subject to export control". Datafusion's full reply is included in Annex 3.

Datafusion confirmed that its product sales are subject to dual-use export licences. In addition, Amnesty International notes that its German corporate entity is bound to the EU's export controls, which should consider the human rights implications of authorizing an export licence for such potentially harmful technology. Being based in Germany also means that Datafusion is recommended to follow the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct.

As Datafusion has declined to answer questions about specific licences, and the UAE does not publish information on export licences, Amnesty International is not able to fully determine what licences were sought or granted, or on what basis. However, since Datafusion exported LIMS products to Pakistan via the UAE, then it is likely that export licences would be required. This is because the UAE, although not a signatory, aligns its export regulations with the Wassenaar Arrangement, which seeks to promote transparency in the sale and export of arms and dual-use items. However, adherence without formal membership undermines transparency, accountability and equal influence in shaping the export control norms that the Wassenaar Arrangement governs.

In addition to seeking information on its sales to Pakistan and related export licences, Amnesty International's letter to Datafusion focused on three areas of concern: their approach to human rights due diligence; their lack of a public grievance capability; and a lack of transparency around their ethics committee, which has existed since at least 2021 in some capacity and from which the company claims to draw its human rights expertise.[265]

In response, Datafusion stated that:

> "We have a panel of ethical consultants analyzing potential future markets and regularly reviewing our existing business covenants. The panel includes 3 independent human-rights experts. We routinely refuse business from countries or entities that are subject to sanction and for those countries where there is a concern about possible misuse of our systems the committee performs an extensive review. All of our customer contracts include a clause that requires our customers to agree to the ethical use of our products including the protection of human rights. We are putting a formal whistleblower policy in place to allow anyone to report potential abuse of our products and we will be initiating training in human-rights observance for all of our own staff from Q1 2025 in addition to the compliance training that we already require all of our employees to attend annually."

Although Amnesty International had sent this inquiry to Datafusion's email address, the company replied from a Protonmail email address that was specifically generated to reply to the email from Amnesty International. Amnesty International was able to confirm this as it retrieved the Pretty Good Privacy (PGP) key for the email address through the Protonmail PGP keyserver. The PGP key shows that the email address was generated on 4 October 2024, the day that Amnesty International received the email.[266] Neither the email or the attached document included a sender's name, and the attached document included a handwritten signature that was illegible. Thus, while Amnesty International did receive a reply, the lack of a specific contact person at the company has made it challenging to develop a fluid channel of communication with the company on these human rights concerns. Amnesty International concludes that

[265] Trovicor's ethical committee report from 2021 where it mentions which deals they declined to take because of human rights risks. Archived by the Internet Archive. Trovicor, *Annual report of the Ethical Committee 2021*, https://web.archive.org/web/20231010125705*/https://trovicor.com/wp-content/uploads/ethical-committee-report-2021.pdf.pdf (retrieved on 10 October 2023). (accessed on 25 August 2025)

[266] The PGP key was retrieved using this web service from Protonmail and importing the PGP key that reveals when the key was generated. Protonmail generates the PGP key when the account gets created. https://mail-api.proton.me/pks/lookup?op=get&search=datafusion@proton.me (accessed on 4 October 2024)

there exists no institutionalized mechanism at Datafusion to deal with such queries in a manner that is transparent and not ad hoc.

Around the time that Datafusion sent this email, the ethical committee report from 2021 was deleted from Trovicor's website, along with its "commitment to human rights" page, both of which had been accessible from at least 2022 to September 2024.[267] As Datafusion was in the process of a name change from Trovicor to Datafusion, it is possible that these changes could have been part of the sunsetting of the Trovicor brand. Datafusion also did not reply to questions about who led its ethics committee, following a commitment in its ethical committee report from 2021: "In 2022 Trovicor will also add an internationally recognized human rights expert to the committee to provide independent oversight of our decisions".

While the Trovicor website confirmed in September 2024 that it had a whistleblowing policy in place, Amnesty International's attempt to use the grievance email address provided in this policy failed to produce a response. Datafusion replied on 4 November 2024 that it was still working on putting the whistleblowing policy in place and that it would launch in early 2025.[268]

In early 2025, Datafusion published revised whistleblower and human rights policies on its website.[269] While it remains unclear who sits on the human rights committee that prepared this document, Amnesty International analysed the metadata of the Word document "Whistleblower Mechanism User Guide" attached to the whistleblower page on Datafusions' website.[270] We found that two of the authors were "CANADIAN LAWYER 1" and "CANADIAN LAWYER 2". It remains unclear whether these human-rights lawyers are part of the ethics committee. Amnesty International knows they're both human rights lawyers as that's how they profile themselves on their website or practise website.

Although a revised whistleblower policy has been shared on its website, the failure to provide an accessible and functional human rights compliant whistleblowing policy and mechanism calls into question the extent to which Datafusion has fulfilled its human rights responsibilities. Moreover, the response to Amnesty International's research letter reinforces that, after years of claiming it had a functional human rights compliant mechanism, the company continues to fall short of abiding by its own human rights commitments.

Amnesty International also sent an email to Datafusion's trovicor domain grievance address.[271] Amnesty International received an automated "bounce" response saying the email address does not exist. Amnesty International then tried sending the same email to a non-published grievance address at Datafusion's new webdomain,[272] which did not receive a bounce and therefore likely went through. However, Amnesty International did not receive any response nor acknowledgement of receipt. While a 2025 webpage on the Datafusion website states that it has a dedicated email address for grievances, it is not publicly accessible on its website.

Questions were asked by a German Greens parliamentarian on both 25 October 2024[273] and 6 December 2024[274] on export licenses issued to Datafusion. In both cases, the German state secretary responded: "that it does not issue on the number of export licenses granted to individual companies in order to protect trade and business secrets".

Given the extensive, publicly available information on surveillance abuses in Pakistan, as well as the numerous allegations of abuses linked to Trovicor/Datafusion's products, which the company does not appear to have taken meaningful steps to address or respond to, it appears that Datafusion is unable or unwilling to conduct adequate due diligence – including by exercising leverage – that is adequate to ensure that its products are not linked to such human rights abuses. Amnesty International believes that Datafusion should halt all exports to Pakistan until it is clear that sufficient safeguards are in place in Pakistan to prevent their use in human rights abuses.

[267] Trovicor, "Our commitment to human rights and the ethical use of our products", https://web.archive.org/web/20231010164226/https://trovicor.com/wp-content/uploads/commitment-to-human-rights.pdf (retrieved on 26 August 2022). (accessed on 25 August 2025)
[268] Trovicor,"Our commitment to human rights and the ethical use of our products" (previously cited).
[269] Datafusion, Whistle Blower Policy, https://datafusion.ai/whistle-blower-policy/ (accessed on 19 August 2025).
[270] Datafusion, Whistle Blower Policy (previously cited).
[271] Datafusion, grievance e-mail address, https://web.archive.org/web/20240508151338/https://trovicor.com/about-us/ (accessed on 25 August 2025)
[272] The grievance address Amnesty International sent an email to is: grievance@datafusion.ai

6.3 HUMAN RIGHTS RESPONSIBILITIES OF GEEDGE NETWORKS AND CEC SUBSIDIARIES LIKE ELINC CHINA CO. LTD

Geedge Networks is a technology company based in China. Section 4.1.1 outlines evidence that Geedge Networks' technologies were exported to Pakistan for use in the WMS. The shipments were delivered by a Chinese state-owned subsidiary, ELINC, as revealed through trade data.

Amnesty International wrote to both Geedge Networks and ELINC in August 2025 to ask about the specific evidence of the shipment of their products to Pakistan, as well as asking the companies to outline their human rights due diligence policies and any grievance or whistleblowing policies. Amnesty International could not find evidence of any human rights, grievance or whistleblowing policies on the websites of Geedge Networks or ELINC.

Amnesty International also asked both companies about any licences for which they had applied for the technologies they exported, but did not receive a reply.

Given the extensive, publicly available information on human rights violations related to censorship in Pakistan, including total internet shutdowns, it appears that Geedge Networks and ELINC have not been able or willing to conduct adequate due diligence – including by exercising leverage - to ensure that their products are not contributing to such human rights abuses. Therefore, Amnesty International believes that Geedge Networks and ELINC should halt all exports to Pakistan related to the WMS until it is clear that sufficient safeguards are in place in Pakistan to prevent their use in human rights abuses. Amnesty International also believes Geedge Networks and ELINC should adopt, implement and publish human rights due diligence policies that establish how they will seek to identify risks and prevent their products being linked to such abuses in the future.

6.4 HUMAN RIGHTS RESPONSIBILITIES OF NIAGARA NETWORKS

Niagara Networks is a technology company headquartered in the USA. Evidence outlined in section 4.5.1 reveals that Niagara Networks equipment was shipped from the USA and the UAE to Pakistani companies involved in the WMS. In section 4.3.1 Amnesty International also shows that Niagara Networks products used for WMS 1.0 have been repurposed for WMS 2.0.

Niagara Networks' website contains no information on whether its products are export controlled. However, without a robust framework for assessing to whom its products are sold, how they are deployed and under what political or legal conditions, Niagara Networks risks being linked to human rights abuses. This absence of safeguards violates the UN Guiding Principles, which emphasize the corporate responsibility to proactively assess and mitigate adverse human rights impacts across their value chains.

Additionally, as Niagara Networks is based in the USA, it is recommended to abide by the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. The USA is also a signatory to the Wassenaar Arrangement.

Amnesty International wrote to Niagara Networks in August 2025 to ask about the specific evidence of the shipment of their products to Pakistan, as well as asking the company to outline their human rights due diligence policies and any grievance or whistleblowing policies. Niagara Networks did not answer Amnesty International's detailed questions but did respond:

> "NN is a bootstrap startup based in Silicon Valley with a total of six sales people worldwide. We follow United States export guidelines strongly. Please note that oftentimes we do not know the end customers and how our products are utilized. Please also note that we only provide the TAP and aggregation function but not the inspection or monitoring. Our products are primarily used in the financial, healthcare & energy markets."

Amnesty International could not find evidence of any human rights, grievance or whistleblowing policies on the website of Niagara Networks. Given the extensive, publicly available information on human rights violations related to mass-surveillance and censorship in Pakistan, including total internet shutdowns,

Amnesty International believes that Niagara Networks should exercise due diligence - including by exercising leverage – to ensure that its products are not linked to such human rights abuses and to prevent adverse impacts of their operations. Should these measures fail to prevent or mitigate such harms, then Niagara Networks should halt all exports to Pakistan or for use in Pakistan, until it is clear that sufficient safeguards are in place in Pakistan to prevent their use in human rights abuses. Amnesty International also believes Niagara Networks should adopt, implement and publish human rights due diligence policies that establish how they will seek to identify risks and prevent their products being linked to such abuses in the future.

6.5 HUMAN RIGHTS RESPONSIBILITIES OF TELECOMMUNICATIONS PROVIDERS IN PAKISTAN

The operation of the mass surveillance system, LIMS, and the national firewall, WMS, requires cooperation from telecommunications providers in Pakistan. Section 3.2.2 outlines how LIMS is enforced at the telecommunications provider level through licensing agreements between the telecommunications providers and the PTA. Similarly, all telecommunications providers are required to install monitoring systems. These monitoring systems allow state agents, including officials from the ISI, to inspect all the data obtained through the LIMS system. This includes obtaining information on surveillance targets, including who they call and for how long, what websites they visit, and where they are located.

Telecommunications providers in Pakistan operate in an extremely challenging context. They are required by law to respond to interception requests from the government. As one employee told Amnesty International "we cannot refuse requests for information if they come from the military".[275] However, the human rights risks posed by such direct access systems, as well as the need for safeguards against abuse, are well known and have been widely recognized by human rights organizations, the UN High Commissioner for Human Rights,[276] as well as industry actors.[277] In the case of Pakistan, by providing direct access to their systems without requiring any form of warrant, telecommunications providers are failing to respect their international human rights responsibilities as well as standards in local laws including the Fair Trial Act and standard operating procedures.

Further, the lack of transparency regarding the acquisition and deployment of technologies by telecommunications providers has deprived users of a full understanding of the ways in which their data can be monitored. Under international human rights standards and their legal obligations under domestic laws, these companies should develop protocols that ensure transparency and mitigate human rights harms that might occur. Currently, there is minimum disclosure from these companies regarding the number and nature of government requests received and complied with.

Furthermore, under the UN Guiding Principles, these companies have a responsibility to conduct human rights due diligence to identify, prevent and mitigate the human rights concerns emerging from LIMS.[278] Such measures could include – at a minimum – encouraging the government to adopt rights-respecting legal and regulatory frameworks, carefully scrutinising government requests to monitor user data or restrict content to ensure their compliance with domestic and international law and standards, challenging government orders that conflict with these legal norms, and providing public transparency regarding any such requests, and decisions and actions taken in relation to them. It is currently unclear whether any telecommunications provider has conducted such due diligence and whether further due diligence has been done as Pakistan has expanded its censorship and surveillance capacities through acquisition of the technologies outlined in this report.

---

[275] Interview by secure voice call with employee at internet service provider in Pakistan, March 2025.

[276] "Because shutdowns have a direct impact on the human rights of all those deprived of communications channels, it is vital that companies' human rights policies address shutdowns by anticipating risks through due diligence processes before entering markets and by adopting mitigation and transparency measures. Companies should explore all lawful measures to challenge the implementation of disruptions. Transparency is critical to stopping shutdowns and limiting their harmful consequences. Companies implementing or affected by restrictions are often the first, and sometimes the only, ones able to share accurate information on the nature of a shutdown and its scope. Therefore, clearly established practices for documenting and escalating demands within companies are vital to ensuring that information is quickly and effectively assessed." United Nations High Commissioner for Human Rights, "Internet shutdowns" (previously cited).

[277] Global Network Initiative, "Defining Direct Access", 3 June 2021, https://globalnetworkinitiative.org/defining-direct-access/
Human Rights, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights. (accessed on 25 August 2025).

[278] Guiding Principles on Business and Human Rights: Implementing the UN "Protect, Respect and Remedy" Framework", 1 January 2012, Principle 15

Lastly, these companies must meaningfully engage potentially affected groups and local civil society, particularly digital rights organizations, to develop an understanding of the human rights impacts of these technologies and create policies to mitigate these harms.[279]

6.6 HUMAN RIGHTS RESPONSIBILITIES OF WMS SUPPORT COMPANIES IN PAKISTAN

The implementation, support and maintenance of WMS firewalls relies on companies located in Pakistan, as outlined in section 4.5. Amnesty International has identified the following companies as being involved in the procurement of equipment for use in WMS 1.0 and/or WMS 2.0:

- A Hamson Pvt Ltd (A Hamson)
- ELC Solutions Corp Pvt Ltd (ELC Solutions)
- Inbox Business Technology Pvt Ltd (Inbox)
- SN Skies Pvt Ltd (SN Skies)

Trade data reveals that each of these companies appears to have received shipments of products that might have been used in the WMS (see Annex 2). In the case of A Hamson, Amnesty International uncovered WeChat conversations between A Hamson and Geedge Networks engineers in the Geedge dataset discussing issues faced by WMS 2.0.

These companies must have had knowledge of how the WMS was set up and its purpose, for example through public tender documents.

Given the extensive, publicly available information on human rights violations related to censorship in Pakistan, including total internet shutdowns, Amnesty International believes that that ELC Solutions, Inbox, SN Skies and A Hamson should urgently examine whether they can take measures to prevent being linked to human rights abuses through their maintenance and support to the PTA for the WMS, and if not, should cease such operations, pending clear evidence that such abuses have ceased and sufficient safeguards are in place to prevent their recurrence.

Amnesty International also believes ELC Solutions, Inbox, SN Skies and A Hamson should adopt, implement and publish human rights due diligence policies that establish how they will seek to identify risks and prevent their support being linked to such abuses in the future.

[279] Guiding Principles on Business and Human Rights (previously cited), Principle 18.

7. CONCLUSION

Mass surveillance and unlawful censorship by the Pakistani authorities – enabled by technology from companies in Canada, China, the UAE and Germany, U.S. and France – represent systemic abuses of fundamental human rights.

Surveillance technologies have enabled the state of Pakistan to monitor, silence and repress dissent, often without legal justification or with lax oversight. The operator of the LIMS system has the capacity to track the location of phones, intercept calls and text messages and track the internet metadata on internet traffic of users simply by inserting phone numbers. The ability to see internet metadata allows the LIMS operator to see what websites a user visits, even if the content or specific pages are encrypted. That the government has such a system in place to carry out mass surveillance of more than 4 million people at any given time within the country, without the need for warrants from a judge, violates not only Pakistan's Fair Trial Act but also international human rights law and standards. As well as being a violation of the right to privacy, mass surveillance creates a chilling effect in society, whereby people are deterred from exercising their rights, both online and offline. International states and companies implicated in the trade, deployment and/or maintenance of this system have so far failed to adequately address their roles.

Internet censorship has been enabled since 2018 by two iterations of the WMS, a firewall system developed, traded and deployed by Canadian, Chinese and US companies. While Sandvine, now Applogic Networks, has stated that it will divest from operating in Pakistan, Amnesty's International's research shows that once such powerful products are exported, they can be repurposed by another company, in this case Geedge Networks, in the next iteration of the WMS setup. Through such re-purposing, companies exporting highly powerful surveillance or censorship technologies are at risk of being linked to human rights violations, even after they have stopped any commercial relationship with a country.

The routine use of internet shutdowns has created an environment where authorities can arbitrarily decide, without any transparency, when a website is added to a block list or removed from it, creating a chilling effect on civil society, disproportionally targeting marginalized communities.

International companies and exporting states bear significant responsibility for allowing this to happen. Alongside the spyware crisis affecting civil society, Amnesty International and other civil society organizations have uncovered a growing crisis that began more than a decade ago: the unbridled export of mass surveillance and censorship technologies used against civil society. The failure to conduct robust human rights due diligence by international companies, and the failure of states to mandate it, coupled with non-transparent export practices, has facilitated the proliferation of both surveillance tools and off-the-shelf equipment that aids these tools. As a result, the rights to privacy, freedom of expression, access to information and a host of other human rights are at risk. The repurposing of surveillance hardware across multiple systems in Pakistan illustrates the enduring risks posed by these technologies.

To uphold international human rights standards, these companies should use all leverage to prevent adverse impacts of their operations. Should they be unable or unwilling to do so or should this leverage fail to prevent or mitigate such harms, then these companies should halt all exports to Pakistan until it is clear that sufficient safeguards are in place in Pakistan to prevent their use in human rights abuses.

States must strengthen export control regimes and enforce transparency in the surveillance technology trade. Pakistan must reform its legal framework, establish independent oversight mechanisms, and ensure meaningful consultation with civil society.

Without urgent action, the unchecked expansion of digital repression in Pakistan will continue to erode civic space and democratic freedoms. This report calls on governments and companies to act decisively to protect human rights and prevent further harm.

8. RECOMMENDATIONS

8.1 RECOMMENDATIONS FOR THE GOVERNMENT OF PAKISTAN

The Government of Pakistan should:

- Refrain from using the Lawful Intercept Management System (LIMS) in its current form. Any surveillance technologies deployed must not engage in mass surveillance and should only be used once binding human rights safeguards, capable of preventing abuse, are in place.
- Ensure that any use of LIMS, or other surveillance technologies, meets international human rights standards around surveillance, including – at a minimum - that:
    - Surveillance is governed by precise and publicly accessible laws.
    - Surveillance affects only specified persons, is authorized by a competent, independent and impartial judicial body and that such authorization includes limitations on time, manner, place and scope of surveillance.
    - Authorized digital surveillance is subject to detailed record keeping, in accordance with documented legal processes for a warrant, and targets are notified as soon as practicable without jeopardizing the purpose of surveillance.
    - Agencies authorized to conduct surveillance and judicial authorities authorizing them prepare meaningful assessments to ensure that the objectives of surveillance could not be achieved with means that pose fewer risks to human rights.
- Ensure that the Pakistan Telecommunications Agency (PTA) immediately ceases the practice of allowing "designated agencies" to use monitoring centres to directly put users under surveillance without oversight or safeguards. Further, the PTA should refrain from imposing undue obligations on telecommunications providers that facilitate mass surveillance.
- Pass legislation on protection of personal data and communications through an inclusive, open and consultative process and ensure that the law is in line with international human rights standards.
- Amend sections 8(2)(c) and 54 of the Pakistan Telecommunication (Re-Organization) Act 1996 to bring them in line with international human rights law which ensures proportionality and provide specific and clear criteria for internet shutdowns.
- Clearly outline, in compliance with international human rights law obligations, limits to restrictions on access to the internet in legislation, including:
    - Restrictions must be based on specific, clear and publicly accessible law.
    - Restrictions must be necessary (that is, the least restrictive option) to achieve a legitimate purpose, as defined in international human rights law.

    - Restrictions must be proportionate and be as narrowly limited as possible in scope and duration.
    - Restrictions must be subject to prior authorization by a court or another independent adjudicatory body, to avoid any political, commercial or other unwarranted influence.
    - Restrictions should be communicated in advance to the public and to telecommunications providers with a detailed and clear explanation of the scope, duration and legal basis, including which services are affected and how.
- Revise laws, through an open and inclusive consultative process, restricting online access to information and freedom of expression, particularly sections 37 and 2R of the Prevention of Electronic Crimes Act 2016 which provide legal justification for censorship through the WMS and national firewall system, in line with international human rights law, and ensure robust safeguards on the rights to privacy and freedom of expression.
- Establish independent, effective and transparent oversight mechanisms of surveillance practices and online censorship requests through enactment of legislation or amendments to existing legislation. It must also be ensured that blanket secrecy rules and national security caveats do not prevent such oversight mechanisms.
- Refrain from using the Web Monitoring System (WMS), or any similar technology, to impose blanket restrictions on internet access under any circumstances.
- Desist from using internet shutdowns and any restrictions on internet access that are incompatible with international human rights law to clamp down on human rights in the future.
- Cease efforts to block, ban or criminalize the use of VPNs or other anonymity tools, as doing so creates a disproportionate and unjustifiable restriction on rights including the right to privacy.
- Enact legislation in line with international human rights law that recognizes the fundamental role that the internet plays in the exercise of human rights and which guards against shutdowns.
- Conduct an independent, impartial and transparent investigation into the purchase of the surveillance and censorship technologies documented in this report and provide avenues for remedy so that affected individuals and communities can seek remedy in practice for violations.
- Publicly share information of all purchase and deployment of surveillance technologies by government and state bodies, including names of companies and purchasing authorities, for all previous, current or future contracts through proactive disclosures and by complying with requests under right to information laws.
- Pass mandatory human rights due diligence law that requires all companies adequately address all possible and actual adverse impacts that their operations, products and services may have along the entire value chain, including rights holders. This law should ensure that this human rights due diligence is conducted early in the process and on an ongoing basis, given that risks and impacts may shift over time.
- Ensure meaningful consultation with civil society organizations, human rights defenders and activists, especially those from marginalized communities, in the process of any policy development, new legislation or legislative review, and its implementation and monitoring.
- Respond positively to pending requests from UN Special Procedures, particularly from the Special Rapporteur on freedom of peaceful assembly and of association, to visit Pakistan. Issue an invitation to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the right to privacy to visit Pakistan.

8.2 RECOMMENDATIONS TO COMPANIES SUPPLYING SURVEILLANCE AND CENSORSHIP TECHNOLOGIES TO PAKISTAN

Amnesty International recommends that companies documented in this report as either producing or exporting surveillance and censorship technologies to Pakistan should:

- Immediately cease the sale and export (and associated maintenance or support) of surveillance and censorship technologies to Pakistan unless it can be demonstrated that your company has exercised due diligence to prevent contributing to human rights harms, including that sufficient safeguards are in place to ensure that these tools are not involved in human rights violations.
- Develop, adopt and make public human rights policies that adhere to international human rights law and standards, and ensure that the policy applies to all subsidiaries, partners and companies along the value chain, including States and companies that may purchase and use these products.
- Ensure transparency regarding sale and use of surveillance and censorship technologies through publicly available human rights due diligence reports and customer lists based on international human rights standards.
- Conduct human rights impact and risk assessments prior to, during and following of deployment of surveillance and censorship technologies to ensure that these tools are not involved in human rights abuses. This should apply to all proposed use, sales and transfers, as well as include engaging with rights holders. The human rights due diligence process should also be transparent.
- Incorporate into any potential future contracts with States and other companies the requirement that these entities respect human rights in the handling of its operation, product or service. This should include the ability to monitor to where this technology would be disbursed, how it would be used and by whom, for the purposes of analysing any possible adverse human rights impacts with which its product may be involved. If these requirements are not met, companies should responsibly disengage from this business relationship.
- Develop accessible and safe grievance mechanisms through which complaints regarding the technology and its use can be addressed effectively. These mechanisms should be available in all countries and measures must be taken to ensure the mechanism is accessible to all, including internally, and that policies are in place to protect whistleblowers.

8.3 RECOMMENDATIONS TO STATES FROM WHICH SURVEILLANCE AND CENSORSHIP TECHNOLOGIES HAVE BEEN EXPORTED

Because of the lack of transparency over the sale and transfer of surveillance and censorship technologies globally, it is not possible for Amnesty International to be certain which countries have granted licences for, or otherwise allowed the export of surveillance and censorship technologies to Pakistan. Nevertheless, based on the evidence outlined, it is likely to include at least the following countries: Canada, China, Germany, the US and the UAE. These countries should:

- Audit any relevant export licences granted to any of the following companies: Geedge Networks, Sandvine/Applogic Networks, Utimaco, Datafusion and Niagara Networks. This should include an independent, impartial, transparent investigation to determine the extent of any unlawful targeting or surveillance transfers, and the offer of remedy, to culminate in a public statement on the results of efforts and steps to prevent future harm.
- Revoke export licences for transfers that pose risks to human rights that cannot be mitigated or prevented.
- Ensure strong enforcement of export control regulations for all surveillance and censorship technologies.

- Ensure that surveillance companies conduct human rights due diligence in relation to their operations, including on the use of their products and services by other companies beyond the first tier in their value chain.
- Take meaningful steps to ensure transparency and accountability regarding human rights due diligence regulation and practices, including by granting public access to beneficial ownership information of companies registered in their jurisdiction.
- Pass mandatory human rights due diligence law that requires all companies adequately address all possible and actual adverse impacts that their operations, products and services may have along the entire value chain, including rights holders. This law should ensure that this human rights due diligence is conducted early in the process and on an ongoing basis, given that risks and impacts may shift over time.
- Enforce a ban on the use or transfer of highly invasive spyware, the functionality of which cannot be limited to only those functions that are necessary and proportionate to a specific use and target, or the use of which cannot be independently audited.
- Implement a human rights regulatory framework that governs surveillance and is in line with international human rights standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer and use of all spyware should be enforced.

SPECIFIC RECOMMENDATIONS TO EU MEMBER STATES FROM WHICH SURVEILLANCE OR CENSORSHIP TECHNOLOGY HAS BEEN EXPORTED:

- European Union (EU) member states, under close monitoring from the European Commission, should ensure the robust implementation of the 2021 EU Export Control Rules and 2024 EU Commission Guidelines, and ensure that exports that threaten human rights are prohibited.
- EU member states must adopt and enforce legislation that requires all corporate actors to respect human rights and implement human rights due diligence measures in line with the UN Guiding Principles. EU member states should require companies to conduct human rights due diligence with respect to the full value chain including the purchase, sale, transfer, export and use of products.
- Ensure that national legislation governing the assessment of export licences takes into account relevant European human rights protections, such as the Charter of Fundamental Rights of the European Union as well as those developed by the Court of Justice of the European Union and the European Court of Human Rights, as well as evidence by civil society and human rights experts.
- The EU and its member states should use all opportunities up to highest level, including summits, visits and regular dialogues on trade, development and human rights dialogues, to raise concerns with the Pakistan authorities about unlawful mass surveillance, and with countries exporting and/or hosting businesses providing surveillance technologies to Pakistan without adequate safeguards.

8.4 RECOMMENDATIONS TO TELECOMMUNICATIONS PROVIDERS IN PAKISTAN

- Carry out adequate human rights due diligence in order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, including in relation to surveillance and internet disruptions, in particular by thoroughly assessing the risks of ordered measures, and making risk assessments public.
- Take all possible lawful measures to prevent government-ordered disruptions from proceeding and, if shutdowns should nevertheless proceed, prevent or mitigate to the extent possible adverse human rights impacts. Exhaust domestic remedies to challenge shutdown requests and implement shutdown requests narrowly, in the most human rights-preserving way, with the goal of keeping communication channels as open as possible.
- Include in their public human rights policy statement their commitment to preventing and mitigating adverse human rights impacts in the context of surveillance and internet shutdowns, and establish

operational policies and procedures in order to be adequately prepared for responding to government requests.

- Publish public transparency reports on requests for access to user data and network shutdown requests from the authorities and notify customers when a network disruption is imminent.
- Reinforce engagement and collaboration with all stakeholders working to prevent and reverse communications disruptions, in particular affected communities and civil society, including by systematically sharing relevant information about communications anomalies and mandated disruptions in a timely manner.
- Develop accessible and safe grievance mechanisms through which complaints regarding the technology and its use can be addressed effectively. These mechanisms should be available in all countries and measures must be taken to ensure the mechanism is accessible to all.

9. ANNEX 1: CONNECTIONS BETWEEN GEEDGE NETWORKS AND PAKISTAN

Section 4.3 presents Amnesty International's assessment, with high confidence, that Geedge Networks has provided firewall technology to Pakistan. This assessment is primarily based on information in the leaked files that documents how Geedge Networks' technologies have been used in Pakistan. However, the leaked files also contain information on meetings between Geedge Networks and officials in Pakistan.

One of the files, "ty-schedule.docx", shows that meetings were scheduled from 31 August 2023 to 2 September 2023 with people from the PTA and other organizations.

Another document, "Schedule.docx", mentions multiple other companies. It is unclear if this was a draft for the same meeting or for a different meeting. PTA and telecoms providers Ufone, Jazz and Pakistan Telecommunication Company Ltd (PTCL) are mentioned.

Amnesty International is also aware of another meeting that happened in early 2024 in Pakistan. A Gmail account can be found within the dataset from an employee of Geedge Networks. Using Ghunt, which is an OSINT method to retrieve account details, Amnesty International can see a Google review of an optician in Islamabad several streets away from the PTA headquarters.

Other documents seen by Amnesty International show an introduction to A Hamson as prepared by Geedge Networks in both English and Mandarin, A Hamson being one of the companies involved in both WMS 1.0 and WMS 2.0. It is unclear whether the meeting with A Hamson took place.

10. ANNEX 2: COMMERCIAL TRADE DATA RECORDS

Amnesty International have been able to obtain commercial trade data from subscription-based trade platforms[280] that sell this data.

10.1 ELC SOLUTIONS CORP (PVT) LTD TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	18.0 KG	OPTICAL LINE PROTECTION BOARD W04805S00 QTY:18-SET NET WEIGHT :337.17-KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER SET (21.09 USD PER KG)	7203.38
2	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	450.0 KG	MULTI MODE FIBRE PATCH CORDS ZTFD-LC-LC-M QTY:450-PAIRS NET WEIGHT:62.50-KGS(AS PER INVOICE & PACKING LIST) DECLARED UNIT VALUE PER PAIR	683.48

[280] The commercial trade platforms that Amnesty International have used consist of: 52WMB and Sayari.

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
					(10.80 USD PER KG)	
3	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	26.0	UNISERVER R4900 G5 QTY:26-SET NET WEIGHT:972.92-KGS(AS PER INVOICE & PACKING LIST)	4296.22
4	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	1.0	UNISERVER R4900 G5 QTY:1-SET NET WEIGHT:32.40-KGS(AS PER INVOICE & PACKING LIST)	1210.73
5	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	10.0 KG	MULTI MODE FIBRE PATCH CORDS ZTFD-MPO-LC QTY:10-PAIRS NET WEIGHT:5-KGS (AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PAIR (18 USD PER KG)	91.13
6	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	144.0 KG	OPTICAL TRANSCEIVER OSNO10N24 QTY: 144-PCS NET WEIGHT:6.48-KGS (AS PER INVOICE & PACKING LIST) DECLARED UNIT VALUE PER PC (1111.10 USD PER KG	7290.41
7	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	1.0	GAP GAP-6000-625BD-ELC QTY:1-SET NET WEIGHT:7.20-KGS(AS PER INVOICE & PACKING LIST)	1640.34
8	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	3.0	UNISERVER R4900 G5 QTY:3-SET NET WEIGHT:110.73-KGS (AS PER INVOICE & PACKING LIST)	6623.86

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
9	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	3.0	NETWORK CONTROL EQUIPMENT 9804-AC-A QTY:3-SET NET WEIGHT:523-KGS(AS PER INVOICE & PACKING LIST)	66539.43
10	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	2.0	SWITCH CE8850-EI-B-BOB QTY:2-SET NET WEIGHT:47.16-KGS (AS PER INVOICE & PACKING LIST)	3337.49
11	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	17.0	COMPUTER SERVER UTR PROBE-40 QTY:17-SET NET WEIGHT:459-KGS (AS PER INVOICE & PACKING LIST)	36452.11
12	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	45.0	UNISERVER R4900 G5 QTY:45-SET NET WEIGHT: 1755.54-KGS(AS PER INVOICE & PACKING LIST)	61280.92
13	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	150.0 KG	SINGLE MODE FIBRE PATCH CORDS ZTFD-LC-LC-D QTY:150-PCS(AS PER INVOICE & PACKING LIST) DECLARED UNIT VALUE PER PC (9.68 USD PER KG)	182.26
14	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	50.0 KG	MULTI MODE FIBRE PATCH CORDS ZTFD-MPO-MPO-M4 QTY:50-PAIRS NET WEIGHT:26.30-KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PAIR (18.76 USD PER KG)	499.7

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
15	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	4.0 KG	OPTICAL TRANSCEIVER OMXD30000 QTY:4-PCS NET WEIGHT:0.08-KGS (AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PC(477.50 USD PER KG	38.68
16	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	80.0 KG	OPTICAL TRANSCEIVER QSFP28-100G-SR4 QTY:80-PCS NET WEIGHT:4.48-KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PC (690.18 USD PER KG	3130.83
17	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	8.0	SWITCH CE5882-48T4S-B QTY:8-SET NET WEIGHT:88.87-KGS(AS PER INVOICE & PACKING LIST)	1797.33
18	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	260.0	CAT6 ETHERNET CABLE HT-TX206-15 QTY:260-PCS NET WEIGHT:110.40-KGS(AS PER INVOICE & PACKING LIST)	434.39
19	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	150.0	UNISERVER R4900 G5 QTY:150-SET NET WEIGHT:4587.45-KGS (AS PER INVOICE & PACKING LIST)	184192.24
20	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	30.0 KG	OPTICAL TRANSCEIVER OSX040N03 QTY:30-PCS NET WEIGHT:2.46-	248.18

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
					KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PC (99.63 USD PER KG	
21	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	50.0	PDU SDPDU-63A-36T QTY:50-SETS NET WEIGHT:175-KGS (AS PER INVOICE & PACKING LIST)	2170.42
22	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	12.0 KG	OPTICAL TRANSCEIVER QSFP-100G CWDM4-LITE QTY:12-PCS NET WEIGHT:0.67-KGS (AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PC (573.85 USD PER KG)	389.11
23	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	3.0	CYBER SECURITY DETECTION EQUIPMENT TAR-AIO-1000E QTY:3-SET NET WEIGHT:60-KGS (AS PER INVOICE & PACKING LIST)	5062.8
24	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	16.0	SWITCH CE6881-48S6CQ-B QTY:16-SET NET WEIGHT:238.73-KGS (AS PER INVOICE PACKING LIST)	12713.83
25	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	656.0 KG	OPTICAL TRANSCEIVER SFP-10G-USR QTY:656-PCS NET WEIGHT:26.24-KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PC (36.50 USD PER KG	969.79

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
26	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	20.0 KG	MULTI MODE FIBRE PATCH CORDS ZTFD-MPO-LC -M4 QTY:20-PAIRS NET WEIGHT:11.40-KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PAIR (18 USD PER KG)	208.39
27	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	3.0	CYBER SECURITY DETECTION EQUIPMENT NFT-5439E QTY:3-SET NET WEIGHT: 126-KGS (AS PER INVOICE & PACKING LIST)	5062.8
28	24 November 2023	Elinc China Co ltd	Elc Solutions Corp Pvt Ltd	6.0	TRAFFIC MANAGEMENT DEVICE CR5P16BUNA71 QTY:06-SETS NET WEIGHT:3232.2-KGS(AS PER INVOICE & PACKING LIST)	423892.52
29	18 January 2025	CHINESE LOGISTICS COMPANY 1	Elc Solutions Corp Pvt Ltd	5.0 KG	SEVER FUSIONCUBE1000 QTY:05-SET NET WEIGHT:166.70-KGS(AS PER INVOICE & PACKING LIST)T)DECLARED UNIT VALUE PER PC (75.487 USD PER KG)	12606.37
30	18 January 2025	CHINESE LOGISTICS COMPANY 1	Elc Solutions Corp Pvt Ltd	18.0 U	PDU SDPDU-63A-36T QTY:18-PCS NET WEIGHT:60-KGS (AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PC (USD 6.432 PER KG)	386.61

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
31	18 January 2025	CHINESE LOGISTICS COMPANY 1	Elc Solutions Corp Pvt Ltd	2.0 U	SWITCH CE5882-48T4S-B QTY:2-SET NET WEIGHT:16.43-KGS (AS PER INVOICE & PACKING LIST)	222.28
32	18 January 2025	CHINESE LOGISTICS COMPANY 1	Elc Solutions Corp Pvt Ltd	1.0 U	TRAFFIC MANAGEMENT DEVICE CR5PI6BUNA71 QTY:01-SETS NET WEIGHT:874.59-KGS(AS PER INVOICE & PACKING LIST)	23815.25
33	18 January 2025	CHINESE LOGISTICS COMPANY 1	Elc Solutions Corp Pvt Ltd	88.0 KG	OPTICAL TRANSCEIVER OSNO10N24 QTY:88-PCS NET WEIGHT:5.09-KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER PC (345.77 USD PER KG	1763.16
34	18 January 2025	CHINESE LOGISTICS COMPANY 1	Elc Solutions Corp Pvt Ltd	8.0 KG	OPTICAL TRANSCEIVER OSX040N03 QTY:8-PCS NET WEIGHT:0.07-KGS(AS PER INVOICE & PACKING LIST DECLARED UNIT VALUE PER PC	12.66
35	18 January 2025	CHINESE LOGISTICS COMPANY 1	Elc Solutions Corp Pvt Ltd	12.0 KG	OPTICAL LINE PROTECTION BOARD WO4805S00 QTY:12-SET NET WEIGHT :83.01-KGS(AS PER INVOICE & PACKING LIST)DECLARED UNIT VALUE PER SET (17.13 USD PER KG)	1424.55

10.2 SN SKIES PVT LTD TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	21 June 2017	Sandvine Inc	Sn Skies Pvt Ltd	42 units	NETWORKING EQUIPMENT	N/A
2	18 February 2021	Niagara Networks	SN Skies Pvt Ltd	3.6 OTHER	03 CONNECTORS BRAND NIAGARA ORIGIN USA QTY 04PC NET WEIGHT 1.5 KGS 02 RACK FOR NETWORKING SWITCH BRAND NIAGARA ORIGIN USA NET WEIGHT 2.10 KGS	60
3	18 February 2021	Niagara Networks	SN Skies Pvt Ltd	1 OTHER	01 NETWORKING BY PASS SWITCH 08 PORTS WITH 2 ADDITIONAL PORTS TYPE 3299TT VOLTAGE 12V BRAND NIAGARA ORIGIN USA QTY01PC NET WEIGHT1.85 KGS	150
4	18 February 2021	Niagara Networks 150 East Brokaw Road California	SN Skies Pvt Ltd	10.0 UNITS	NETWORKING EQUIPMENTS	N/A
5	21 February 2021	Niagara networks Los Angeles	SN Skies Pvt Ltd	N/A	Networking eqpt	N/A
6	23 February 2021	Niagara Networks	SN Skies Pvt Ltd	4	1 HYBRID NETWORKING PACKET BROKER 32 PORTS BRAND NIAGARA ORIGIN USA MODEL 3808MNAC2 WITH STANDARD ACCESSORIES VOLTAGE 100240V CURRENT 21A 2.29AMPS FREQUENCY 5060HZ POW	470

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
7	21 March 2021	Niagara Networks UAE	SN Skies Pvt Ltd	N/A	2847 main chassis ac s2 versi	N/A

10.3 A HAMSON PVT LTD TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	5 July 2019	Sandvine Inc	A Hamson Pvt Ltd	32 units	SANDVINE NETWORKS	N/A

10.4 TELENOR TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	26 October 2014	Trovicor Gmbh	Telenor Pakistan Pravite Ltd	N/A	"Monitoring center equipment"	N/A
2	12 August 2017	Trovicor Solutions Fz LLC	Telenor Pakistan Pravite Ltd	90	"Telenor equipment"	N/A
3	4 May 2021	Trovicor Solutions Fz LLC	Telenor Pakistan Pravite Ltd	1	"LIMS MEDIATION DEVICE FOR ZTE LIG UP TO 400,000 SUBSCRIBERS SOFTWARE,QTY01 PKGES DETAIL INVOICE UPLOADED."	67231,52

10.5 PAK TELECOMMUNICATION MOBILE LIMITED (TRADE NAME UFONE) TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	8 May 2017	Trovicor Solutions Fz LLC	Pak Telecom Mobile LTD	300	"LIMS UPGRADE"	N/A
2	15 February 2019	Trovicor Solutions Fz LLC	Pak Telecom Mobile LTD	1	"LIMS MEDIATION DEVICE	N/A

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION SOFTWARE DVD"	DECLARED VALUE (USD)
3	1 October 2019	Trovicor Solutions Fz LLC	Pak Telecom Mobile LTD	20	"Various computer parts"	N/A
4	7 August 2021	Trovicor Solutions Fz LLC	Pak Telecom Mobile LTD	1	"LIMS DF SERVER WITH ACCESSORIES QTY 01 DETAIL AS PER INVOICE PACKING LIST"	379 046,40
5	17 November 2022	Trovicor Solutions Fz LLC	Pak Telecom Mobile LTD	1	"SOFTWARE ON CD 1 LOT"	1 386 153,85
6	17 November 2022	Trovicor Solutions Fz LLC	Pak Telecom Mobile LTD	15	"SERVER WITH ACCESSORIES VM SERVER SN CZJ2142009 CZJ2250DZT CZJ2250DZV MCNG STORAGE EXPANSION SN XK8001GE XK8001CF XK9001V9 XK9001RX XK9001XT2 XK9001RV XK9001HY XK900"	203 559,68
7	14 June 2023	Trovicor Solutions Fz LLC	Pak Telecom Mobile LTD	1	"SERVER WITH ACCESSORIES DETAIL AS PER INVOICE / PACKING LIST"	2 120 603,74

10.6 CHINA MOBILE PAKISTAN (CMPAK LTD) (TRADE NAME ZONG 4G) TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	13 April 2016	Trovicor Solutions Fz LLC	Cmpak ltd	960	"SHOT GUN PUMP"	N/A

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
2	11 December 2019	Trovicor Solutions Fz LLC	Cmpak ltd	937	“Computer parts servers”	N/A
3	23 December 2020	Trovicor Solutions Fz LLC	Cmpak ltd	0,3	“I UNIT OF LIMS MG MT AND AMP MD SOFTWARE UPGRADE EUR UNIT IC NO ICN202000211 DTD 17 NOV 2020”	N/A
4	23 November 2021	Trovicor Solutions Fz LLC	Cmpak ltd	16	“SERVERS VIRTUAL MACHINE SERVER, DATA BASE SERVER, DEPLOYMENT SERVER, LMS MANAGEMENT SERVER, LOAD BALANCE SERVER, LIMS DF”	348 852,98
5	23 November 2021	Trovicor Solutions Fz LLC	Cmpak ltd	24	“Desktop PC”	64 384,87
6	23 November 2021	Trovicor Solutions Fz LLC	Cmpak ltd	6	“SWITCHES 48 PORT 4 PCS, 24 PORTS 2 PCS ”	106 359,68
7	23 November 2021	Trovicor Solutions Fz LLC	Cmpak ltd	2	“NETWORK EQUIPMENT FIREWALLS”	58 172,35
8	23 November 2021	Trovicor Solutions Fz LLC	Cmpak ltd	42	“Software”	1 199 425,58
9	23 November 2021	Trovicor Solutions Fz LLC	Cmpak ltd	180	“Cables wt 190KG”	9 453,81
10	2 March 2022	Trovicor Solutions Fz LLC	Cmpak ltd	2	“SERVERS MCNG STORAGE SERVER”	205 498,47
11	2 March 2022	Trovicor Solutions Fz LLC	Cmpak ltd	4	“FC switch 16 ports”	18 065,80
12	19 September 2023	Trovicor Solutions Fz LLC	Cmpak ltd	1	“SOFTWARE (NETWORK CONNECTIVITY MODULE) (1/O: CZECH REPUBLIC POLAND	1 463 843,74

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
					GERMANY CHINA UAE and USA"	
13	19 September 2023	Trovicor Solutions Fz LLC	Cmpak ltd	1	"DELL SERVER (POWER EDGE R640 WITH STANDARD ACCESSORIES (VO: CZECH REPUBLIC POLAND GERMANY CHINA UAE AND USA)"	10 889,72
14	31 May 2024	Trovicor Solutions Fz LLC	Cmpak ltd	2	"HP COMPUTER SERVER WITH ACCESSORIES_X000D_ (I/O: CZECH REPUBLIC POLAND GERMANY CHINA UAE USA)"	59 948,62
15	31 May 2024	Trovicor Solutions Fz LLC	Cmpak ltd	1	"SOFTWARE LICENSES IN CD FOR TELECOM INDUSTRY. XOOOD_ (/O: CZECH REPUBLIC POLAND GERMANY CHINA UAE USA)"	959 365,21
16	31 May 2024	Trovicor Solutions Fz LLC	Cmpak ltd	1	"DELL COMPUTER SERVER WITH ACCESSORIES_X000D_ (I/O: CZECH REPUBLIC POLAND GERMANY CHINA UAE USA)"	27 379,14

10.7 CYBER INTERNET SERVICES PVT LTD TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	4	"DATA COMMUNICATION & NETWORKING EQUIPMENT: 10 SM DUAL CORE LR10KM OPTICAL TRANSCEIVERS FOR JUNIPER SR340 ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY: 4 PCS)"	1 011,08

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
2	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	4	"DATA COMMUNICATION & NETWORKING EQUIPMENT: JUNIPER SRX340-SYS-JB ROUTER WITH AC PSU ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY: 4 PCS)"	8 201,32
3	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	61	"DATA COMMUNICATION & NETWORKING EQUIPMENT: CABLES ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY: 61 PCS)"	3 678,30
4	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	6	"DATA COMMUNICATION & NETWORKING EQUIPMENT; LAPTOPS ALONG WITH STANDARD ASSESSORIES AND ATTACHMENTS (QTY: 6)"	10 028,52
5	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	61	"DATA COMMUNICATION & NETWORKING EQUIPMENT: PATCH CORDS WITH TRANSCEIVERS ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY: 61 PCS)"	3 678,30
6	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	10	"DATA COMMUNICATION & NETWORKING EQUIPMENT: LCD SCREENS ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY: 10 PCS)"	1 507,60

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
7	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	2	"DATA COMMUNICATION & NETWORKING EQUIPMENT: JUNIPER SRX550-545AP-M ROUTER WITH DUAL AC PSU ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY: 2 PCS)"	8 442,54
8	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	2	"DATA COMMUNICATION & NETWORKING EQUIPMENT: 3U RACKMOUNT "NAS" SERVER ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY: 2 PCS)"	54 068,50
9	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	19	"DATA COMMUNICATION & NETWORKING EQUIPMENT: DESKTOP SYSTEMS ALONG WITH ACCESSORIES & ATTACHMENTS (QTY: 19 PCS)"	28 644,40
10	31 January 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	3	"DATA COMMUNICATION & NETWORKING RACK MOUNT FIBRE BYPASS SWITCH 3808C NIAGERA NETWORKS WITH SR/LR SFP ALONG WITH STANDARD ACCESSORIES & ATTACHMENTS (QTY 3 PCS)"	183 926,94
11	14 February 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	1	"DATA COMMUNICATION & NETWORKING RACK MOUNT FIBRE BYPASS WITCH 3808C NIAGERA NETWORKS WITH SR/LR SFP ALONG WITH STANDARD	62 506,07

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
					ACCESSORIES & ATTACHMENTS (QTY 1 PCS)"	
12	14 February 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	32	"DATA COMMUNICATION & NETWORKING EQUIPMENT: AMD EPYC 7XXX SERVER ALONG WITH STANDARD ACCESORIES & ATTACHMENTS (QTY: 32PCS)"	652 870,78
13	14 February 2023	Trovicor Solutions Fz LLC	Cyber Internet Sevices pvt ltd	1	"SERVER RACK (QTY: 1)"	204,94

10.8 TROVICOR PAKISTAN PVT LTD TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	26 October 2014	Trovicor Gmbh	Trovicor Pakistan Pravite Ltd	N/A	"Monitoring center equipment"	N/A

10.9 TROVICOR FZ LLC (DF SYSTEMS FZ-LLC) TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	7 June 2014	Trovicor FZ LLC	Warid Telecomm Pvt Ltd	N/A	"Industrial server"	N/A
2	21 December 2016	Trovicor FZ LLC	Trovicor SMC Pvt LTD	N/A	"laptop and accessories"	N/A

10.10 PAKISTAN MOBILE COMMUNICATIONS PVT LTD (TRADE NAME JAZZ, FORMERLY MOBILINK) TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	13 August 2016	Trovicor Solutions Fz LLC	Pakistan Mobile Communication Pvt	1	"LIMS software"	N/A
2	25 November 2020	Trovicor Solutions Fz LLC	Pakistan Mobile Communication Pvt	1077	"Equipments"	N/A
3	1 December 2022	Trovicor Solutions Fz LLC	Pakistan Mobile Communication Pvt	5	"CELLULAR INFRASTRUCTURE EQUIPMENT HARDWARESOFTWARE VM SERVER HP PROLIANT DL360 GEN10 8SFF DETAIL AS PER INVOICE"	98 700,19
4	1 December 2022	Trovicor Solutions Fz LLC	Pakistan Mobile Communication Pvt	15181	"CELLULAR INFRASTRUCTURE EQUIPMENT HARDWARESOFTWARE DECODING HI2 TICKETSLICENSE FOR 1 HI2S DETAIL AS PER INVOICE"	917 378,44
5	2 September 2023	Trovicor Solutions Fz LLC	Pakistan Mobile Communication Pvt	1	"TELECOM EQUIPMENT (PANI DEVELOPMENT WORK_TROVICOR SW)"	175 221,51
6	11 January 2023	Trovicor Solutions Fz LLC	Pakistan Mobile Communication Pvt	1	"SERVERS WITH ACCESSORIES QTY = 1 LOT AS PER INVOICE"	375 361,01
7	11 January 2023	Trovicor Solutions Fz LLC	Pakistan Mobile Communication Pvt	1	"SOFTWARE ON CD QTY = 1 NO AS PER INVOICE"	573 942,27

10.11 INBOX BUSINESS TECHNOLOGIES PVT. LTD. TRADE DATA

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
1	1 February 2016	UAE TECHNOLOGY DISTRIBUTOR 1	Inbox Business Technologies Pvt LTD	2	SANDVINE ADVANCED SUPPORT	N/A
2	2 March 2018	N/A	Inbox Business Technologies Pvt LTD	46	SANDVINE PTS	N/A
3	28 July 2019	Sandvine Inc	Inbox Business Technologies Pvt LTD	760	SANDVINE HARDWARE	N/A
4	23 August 2021	UAE TECHNOLOGY DISTRIBUTOR 2	Inbox Business Technologies Pvt LTD	28	SANDVINE PLATFORM STORAGE SERVER IQ52600, 2RU, 1024GB RAM, 8X25GBE, 2X960GB SSD, 2XPS INCLUDING ALL FOLLOWING OPTIONS	4 443 989,00
5	23 August 2021	UAE TECHNOLOGY DISTRIBUTOR 2	Inbox Business Technologies Pvt LTD	18	SANDVINE EXTERNAL STORAGE UNIT SN1204 STORAGE NODE, 12X4TB HDD, 2RU, REDUCDANT AC POWER SUPPLY INCLUDING ALL FOLLOWING OPTIONS	2 058 126,62
6	23 August 2021	UAE TECHNOLOGY DISTRIBUTOR 2	Inbox Business Technologies Pvt LTD	3	SANDVINE STORAGE SERVER PL1881R740, 384GB, 2XSYS, 2XSFP, 2XPS, 12XHDD INCLUDING ALL FOLLOWING OPTIONS	623 715,00
7	23 August 2021	UAE TECHNOLOGY DISTRIBUTOR 2	Inbox Business Technologies Pvt LTD	2	SANDVINE STORAGE SERVER PL1840, 2RU, 192GB, X710I350, 2XPS INCLUDING ALL FOLLOWING OPTIONS	195 740,12
8	23 August 2021	UAE TECHNOLOGY DISTRIBUTOR 2	Inbox Business Technologies Pvt LTD	20	SANDVINE STORAGE SERVER PL1860, 2RU, 384GB, X710I350, 2XPS INCLUDING ALL FOLLOWING OPTIONS	3 052 222,26
9	26 October 2021	Niagara Networks	Inbox Business Technologies Pvt LTD	18.0 OTHER	100GB FULL BYPASS SEGMENT FIXED MODULE LR4 2	312119.86

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION	DECLARED VALUE (USD)
					NETWORK PORTS AND 2 APPLIANCE PORTS HIGH GRADE INTEGRATED TRANSCEIVERS FOR NETWORK PORTS MODULE OCCUPIES DOUBLE BAY	
10	26 October 2021	Niagara Networks	Inbox Business Technologies Pvt LTD	9.0 OTHER	2825 MAIN CHASSIS AC WITH TWO FIXED CONFIGURATION 100GB BYPASS SEGMENT BAY INCLUDES TWO POWER SUPPLY UNITS AND FOUR FAN UNITS INTEGRATED NON BLOCKING SWITCHING FABRIC AND HEART B	62586.54
11	26 October 2021	Niagara Networks	Inbox Business Technologies Pvt LTD	36.0 OTHER	100GBASE SR4 100M QSFP28 OPTICAL TRANSCEIVER	40321.98
12	1 February 2022	UAE TECHNOLOGY DISTRIBUTOR 2	Inbox Business Technologies Pvt LTD	9	SANDVINE PLATFORM STORAGE SERVER IQ52600, 2RU, 1024GB RAM, 8X25GBE, 2X960GB SSD, 2XPS INCLUDING ALL FOLLOWING OPTIONS	4 631 847.00
13	22 February 2022	Niagara Networks	Inbox Business Technologies Pvt LTD	108.0 OTHER	100GBASE LR4 10 KM QSF28 OPTICAL TRANSCEIVER	46255.35
14	22 February 2022	Niagara Networks	Inbox Business Technologies Pvt LTD	12.0 OTHER	3296 MAIN CHASSIS USB POWER INPUT SUPPORT UP TO 4 MODULES	15588.55
15	22 February 2022	Niagara Networks	Inbox Business Technologies Pvt LTD	27.0 OTHER	2 PASSIVE BYPASS SEGMENTS LR4LRLX EACH SEGMENT INCLUDES 2 NETWORK PORTS AND 2 APPLIANCE PORTS	6779.74
16	17 February 2022	Niagara Networks	Inbox Business Technologies Pvt LTD	1.0 OTHER	UNDER WARRANTY REPAIR REPLACEMENT PARTS VIDE EXPORT GD NO. 3113 DT 221221 2825 MAIN CHASSIS AC	7316.98

ID	DATE	FROM	TO	QUANTITY	PRODUCT DESCRIPTION WITH TWO FIXED CONFIGURATION	DECLARED VALUE (USD)
17	4 March 2022	Sandvine Corporation	Inbox Business Technologies Pvt LTD	1	UNDER WARRANTY REPAIR REPLACEMENT PARTS VIDE EXPORT KAFE SB1799 DT 02112021 SANDVINE PTS32400 POLICY SWITCH REPAIRING CHARGES USD 350	440,00
18	6 June 2022	Niagara Networks	Inbox Business Technologies Pvt LTD	9.0 OTHER	2 PASSIVE BYPASS SEGMENTS LR4LRLX EACH SEGMENT INCLUDES 2 NETWORK PPORTS AND 2 APPLIANCE PORTS 1G10G25G40G100G	2361.38
19	6 June 2022	Niagara Networks	Inbox Business Technologies Pvt LTD	3.0 OTHER	GOODS FOR DEMONSTRATION PURPOSES 3296 MAIN CHASSIS USB PWOER INPUT SUPPORTS UP TO 4 MODULES	4072.12
20	23 July 2022	Sandvine Inc	Inbox Business Technologies Pvt LTD	1	SANDVINE PLATFORM STORAGE SERVER IQ52600 UNDER WARRANTY REPAIR REPLACEMENT PARTS VIDE EXPORT SB NO. 4331 DT 21032022	350,00
21	5 April 2023	Niagara Networks	Inbox Business Technologies Pvt LTD	1.0	2825 MAIN CHASIS UNDER WARRANTY REPAIR / REPLACEMENT PARTS VIDE VIDE EXPORT GD NO 2881 DTD-01-02-2023	646.09

11. ANNEX 3: COMPANY LETTERS

August 22, 2025

Re: Amnesty International Request for Response and Information on Amnesty International's Research on Surveillance and Censorship Technologies in Pakistan

Dear Amnesty Tech and Amnesty International:

This responds to your recent letter to AppLogic Networks concerning Amnesty International's research on surveillance and censorship technologies in Pakistan. We appreciate the opportunity to engage and respond.

As your letter acknowledges, internet-related technologies can be used responsibly, including for ensuring the effective operability of the internet by, for example, blocking malicious traffic, and other legitimate and lawful purposes. Sandvine Corporation (Sandvine) has not and does not support the misuse of its products and prohibited the use of its products to violate law, regulations, and internationally recognized human rights standards, among other things.

As you are aware, AppLogic Networks is independent from its predecessor, Sandvine (see Sandvine emerges as AppLogic Networks). AppLogic Networks is owned by several US-based entities, none of which is Francisco Partners, the former owner of Sandvine. AppLogic Networks provides software in democratically focused jurisdictions with a consistent, demonstrable commitment to internet freedom and strong rule of law protections and does not provide or sell hardware. Pursuant to a transfer services agreement, AppLogic Networks provides certain services to Sandvine and thus is engaged in this response.

In or around 2017, Sandvine sold hardware and software through one or more partners for use and/or deployment in Pakistan. While we acknowledge prior third-party misuse of Sandvine's products, none of the Sandvine products were controlled for export control purposes and none had or has the capability to decrypt user data (i.e., voice, video, messaging, etc.) or inject spyware. Sandvine was not aware of Geedge Networks as identified in the Amnesty International letter and any hardware repurposed as articulated in the Amnesty International letter is off-the-shelf Dell and Niagara equipment that does not contain any special capability that is unique to Sandvine's solution.

As a matter of historical practice, where Sandvine has become aware of allegations of potential product misuse involving its products, it has conducted an internal review to understand the facts and taken steps to inform and work with its partners and/or customers to detect, prevent, or cease any potential product misuse, particularly as the use of Sandvine products was conditioned upon end user compliance with certain standards, including, but not limited to, complying with laws and regulations and not using

Sandvine products for mass surveillance of individuals or inappropriate internet censorship. Sandvine exited its business in Pakistan in 2023, revoked all licenses to use its products in the jurisdiction, disabled the software, and notified its relevant customers and/or partners of the same. The Sandvine solution sold in the jurisdiction has not been in use since that time.

As a signatory to Access Now's letter to Sandvine dated October 31, 2024 (attached), Amnesty International would have received a copy of Sandvine's contemporaneous response to Access Now as Sandvine requested and received confirmation that its written response dated November 21, 2024 (attached) had been delivered to all Access Now Letter signatories. Accordingly, as you are aware, in Sandvine's written response, it indicated its exit from Pakistan, among other countries. It also noted the significant changes being made to its governance structure and indicated that it was in the process of evolving its human rights due diligence policy and processes. Sandvine also confirmed that it maintained a grievance mechanism accessible to all individuals and organizations to report allegations of potential product misuse. AppLogic Networks also maintains grievance mechanisms, including one that is managed by a third party, allows for anonymous reporting, and can be used by individuals and organizations to report allegations of potential product misuse (see https://report.syntrio.com/applogicnetworks).

AppLogic Networks has a clear commitment to championing human rights and we take this commitment seriously. As such, we share Amnesty International's commitment and efforts to prevent, detect, and mitigate the risk of technology from being misused to violate human rights globally.

We appreciate the opportunity to engage with you on such topics, particularly as the newly formed AppLogic Networks evolves and strengthens its human rights due diligence policy and processes. We also welcome the opportunity to engage further on these important issues going forward.

Thank you.

Carol Tate
Chief Ethics & Compliance Officer

AppLogic NETWORKS
The AppGoE Company

DATAFUSION SYSTEMS

DF Systems FZ LLC | Arjaan Office Tower 907 | Dubai, UAE

AMNESTY INTERNATIONAL

[redacted]

4 November 2024

SUBJECT: RE: AMNESTY INTERNATIONAL RESEARCH ON SURVEILLANCE TECHNOLOGY IN PAKISTAN

[redacted]

I refer to your recent request regarding our Lawful Interception (LI) capabilities.

Datafusion Systems (formerly known as Trovicor Intelligence) is based in the UAE and sells a standards-based, Lawful-Interception (LI), targeted Monitoring Centre (MC) product. We sell to customers all around the world although one of our subsidiaries, Datafusion Systems Gmbh handles business in Europe exclusively. Our customers are law-enforcement or other legally appointed governmental agencies that have the right to perform communication interception for the purpose of evidence gathering to support detection of terrorism or other criminal activity. Our products are sold subject to export control. Due to strict confidentiality agreements we cannot disclose any specific information about our customers, partnerships or end-users.

Technically, the MC only receives intercepted communications from telecom networks over standardised interfaces and has no capability to effect interception in those networks. In order to initiate communications interception a separate mediation platform is required that interfaces directly with network elements (Lawful Interception Management System - LIMS). Datafusion Systems does not manufacture such a LIMS product. The MC can only operate on a targeted basis and each target must be identified by a unique identifier (typically a phone number).

While our products as well as those of our competitors are commonly used by justice departments in all Western countries, we are fully aware that it is extremely difficult to prevent a possible misuse of these solutions and hence we do our very best to minimize this risk.

We have a panel of ethical consultants analyzing potential future markets and regularly reviewing our existing business covenants. The panel includes 3 independent human-rights experts. We routinely refuse business from countries or entities that are subject to sanction and for those countries where there is a concern about possible misuse of our systems the committee performs an extensive review. All of our customer contracts include a clause that requires our customers to agree to the ethical use of our products including the protection of human rights. We are putting a formal whistleblower policy in place to allow anyone to report potential abuse of our products and we will be initiating training in human-rights observance for all of our own staff from Q1 2025 in addition to the compliance training that we already require all of our employees to attend annually.

As stated above, the solutions we sell are used routinely by European judicial and police services. In other geographies, we see competition from other vendors, including those from Russia, China, Europe and Israel, some of whom have no concern for Human Rights whatsoever.

Yours faithfully,

Management, Datafusion Systems.

Datafusion Systems
Arjaan Office Tower 907, Al Sofouh Complex, Dubai Media City, P.O. Box 502859, Dubai, UAE
phone: +971 4 4393470, fax: +971 4 4393471 | info@datafusion.ai, www.datafusion.ai

Statement in response to Amnesty International, letter dated 21 October 2024

In reply to your request for response and information regarding deployment of surveillance technology in Pakistan, we would like to answer as follows:

- We are contractually prohibited from providing information on the specifics of our business partnerships or implementations.
- In everything we do, we fully comply with the relevant applicable legal requirements and export control laws and regulations. This applies to both the strict German and the relevant international requirements.

- We also hold our business partners responsible. This includes that

  - We oblige our resellers and customers to strictly comply with all applicable export and import laws and regulations, including those of Germany and Europe, and any applicable embargo regulations including those of the United Nations.
  - Our export compliance policy and corporate social responsibility guidelines are binding for our business partners and customers.

- In principle, telephone monitoring can always be technically implemented without a LIMS systems. LIMS systems assist telecommunication service providers in complying with electronic surveillance law enforcement orders.

Kind regards,

Utimaco Management Services GmbH
Germanusstraße 4, 52080 Aachen, Germany

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

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.

INDEX: ASA 33/0206/2025
AUGUST 2025
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL