DRF USA

UNVEILING CYBER-SURVEILLANCE TECHNOLOGIES IN SOUTH ASIA

Acknowledgements

This report is an important part of the discourse DRF hopes to foster around the cyber-surveillance in South Asia. These country reports aim to explore the technologies increasingly being deployed to expand digital monitoring and control. The report would not have been possible without the contributions of our esteemed authors including independent researchers from Pakistan and India, Tech Global Institute (TGI), and Factum. DRF would also like to thank the team at FIND.ngo and acknowledge the support and direction provided in putting together this report.

Table of Contents

Introduction 08
Digital Rights Foundation

01 | Pakistan 15
Zuha Siddiqui

Introduction 18

Historical Context 19

Findings 24

- Prevalence of Cyber Intrusion 24
- State Rationale 29
- Major Breaches, Victims and Beneficiaries 31
- External Actors in the Mix 36

Legal Framework 39

- Privacy and Surveillance in the Law 39
- Mohtarma Benazir Bhutto vs President Pakistan 41
- The Move Towards Codifying Cybercrime 44
- Current State Capacity and Response 47

Recommendations 49

Conclusion / Towards a More Balanced Approach 53

Works Cited 55

Introduction 66
Historical Context 69
Findings 75
Victims of Surveillance 75
Surveillance Tools and Systems Used in Bangladesh 78
Intrusive Spyware for Device Surveillance 78
Integrated Lawful Interception System (ILIS) 79
Mobile Phone Surveillance and IMSI Catchers 81
Social Media Monitoring and Online Content Surveillance 82
Digital Forensic Tools 83
Import-Export Data and Trade Pattern in Surveillance Tech 84
Legal Framework & Practice 85
Recommendations 89
Conclusion 91
References 92

Abbreviations 100
Introduction 103
Historical Context 104
Findings on Cyber Intrusion in India 110
Mapping the Deployment of Spyware 110
2019 Pegasus Disclosures 110
2021 Pegasus Disclosures 112
Apple Threat Notifications 114
Victims of Spyware 115
Mapping the Response of the Union Government 116
Apple Threat Notification 119
Mapping Responses of State Governments 121
Legal Framework 124
Information Technology Act, 2000 125
The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 125
CERT-In Cybersecurity Directives (2022) 126
Digital Personal Data Protection Act, 2023 127
Indian Telecommunications Act, 2023: Re-legislating Colonial Provisions 128

Judicial Oversight and Surveillance Frameworks 129
Judicial response to Pegasus revelations 130
Findings of the Technical Committee 133
Pegasus Hearings — Latest Dispatch From 2025 134
Recommendations 136
Confronting Unlawful Deployment of Cyberintrusion Technologies in India: Gaps, Opportunities, and Pathways Forward 136
Opportunities for Transnational Accountability 136
Building a Resilient Ecosystem Through Capacity Building 137
Engaging in Global Norm-Shaping Forums 137
Civic Education Campaigns to Reframe Privacy as a Constitutional Right and Counter Prevailing Indifference to Surveillance in South Asia 138
Strategic Litigation as a Tool for Structural Change 138
Conclusion 139

04 | **Sri Lanka** 152
Prihesh Ratnayake & Omar Rajarathnam

Abbreviations 153
Introduction 155
Historical Context 157
Findings on Surveillance in Sri Lanka 163
The Evolving Landscape of State Surveillance 163
Historical Context of State Surveillance in Sri Lanka 163
Efforts to Gain Access to Modern Digital Surveillance Technology 164
Evidence of Spyware Procurement and Interest 165
Domestic Surveillance Development 167
Telecommunications Technology with Foreign Components 168
The Impact of Foreign Influence on State Surveillance 169
Perceptions on State Surveillance in Sri Lanka 171
Legal Framework 173
Sri Lanka's Fractured Cyber Surveillance Framework 173
The Personal Data Protection Act (PDPA): A Step Towards Accountability? 176

05 | **Analysis and Conclusion** 189
Digital Rights Foundation

Appendix 199

Executive Summary

Introduction

Surveillance has, for over centuries, been employed by the state to cheat, manipulate and blackmail politicians, judges, journalists, activists and even private individuals. And while the method may have changed as technology is advancing and becoming more sophisticated, the end remains the same: exploitation for personal and political gain. Where once it was wiretapping an executive's office, now it is the stealthy installation of invasive malware and software into personal devices, including mobile phones, laptops, desktops or any other electronic device.

Tools for surveillance today, can fall into multiple types and categories, and given this multifaceted aspect of surveillance tools and technology today, it is necessary to briefly delve into what these tools include, what they're categorized as and why geographical context is important when talking about the kinds of tools and capabilities being used.

Today, the term 'spyware' - used interchangeably with the term 'cyber-intrusion' - is widely evoked everywhere and has effectively become a buzzword, especially in the development sector to include any and all infringements that fall under the online tracking, monitoring, and/or recording of an individual's personal information. While applied rightfully so, given the increase in human rights violations that involve surveillance tactics and technology, these terms don't necessarily mean the same thing or can be applicable in every surveillance infringement. According to the Stockholm International Peace Research Institute (SIPRI), cyber-surveillance tools associated with the systematic observation of persons can be divided into two categories: those that allow interception and those that involve device compromise.[1] Spyware, consequently, is a sub-category of cyber-surveillance that specifically deals with '[tools] that can be inserted into electronic devices without detection and used to remotely monitor them.' Ranging from more accessible and widely available lawful interception to more complicated technology that involves remotely controlled spyware as well as digital forensic systems - the surveillance market is a largely diverse and marketable area in today's cyber world.

---

[1] SIPRI 'Mapping the location of manufacturers of spyware and other cyber-surveillance tools,' Stockholm International Peace Research Institute, September 2025, https://www.sipri.org/visualizations/2025/mapping-location-manufacturers-spyware-and-other-cyber-surveillance-tools

For the use of this research, we will be focusing on lawful interception, mobile phone interception and data retention systems - all of which exploit existing fundamental rights of privacy and freedom of expression. As research and its subsequent case studies stand to show, surveillance in the Global Majority is more complex and less straightforward than modern definitions in the age of technology. While recent innovations and advancements in surveillance are being employed by companies across the world to monitor individuals, existing technology is more often than not being tweaked, changed and adapted to fit the purpose of close observation.

In July 2021, an investigation by Forbidden Stories and Amnesty International called the Pegasus Project, shook the world. It revealed how Pegasus, a military-grade spyware software, had been used to target at least 189 journalists, 85 human rights defenders, and over 600 politicians and government officials globally, including active cabinet ministers and diplomats in various states.[2]

Since then, several other cases of explicit, unlawful surveillance have cropped up all over the world, including unauthorized surveillance of citizens in Myanmar[3], illegal storage of personally identifiable information of Palestinians in Gaza[4] and multiple privacy breaches originating from NSO Group across platforms such as Meta that have left individuals' personal data vulnerable.[5]

[2] "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally," Amnesty International, July 19 2021, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[3] "Norwegian Telecom Telenor allegedly shared personal data with Myanmar military junta," Business & Human Rights Center, August 20, 2025, https://www.business-humanrights.org/en/latest-news/norwegian-telecom-telenor-allegedly-shared-personal-data-with-myanmar-military-junta/

[4] Harry Davies and Yuval Abraham, "'A million calls an hour': Israel replying on Microsoft cloud for expansive surveillance of Palestinians," The Guardian, August 6 2025, https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud

[5] "Winning the Fight Against Spyware Merchant NSO," Meta, May 6 2025, https://about.fb.com/news/2025/05/winning-the-fight-against-spyware-merchant-nso/

These incidents created not just a combined moment of reckoning—it sparked a global demand for accountability, transparency and most importantly, investigation. Since these revelations have become public, we've seen movement: the U.S. blacklisted NSO Group[6] and other surveillance firms; the UK and French governments launched a multistakeholder initiative called the Pall Mall Process[7] earlier this year that prioritizes cross border collaboration between states and cyber-intelligence companies to tackle the proliferation of cyber intrusive technologies, creating a global world order that sets important precedents to hold states and firms accountable. Though narrow in their focus on what constitutes as “cyber intrusive technologies" and limited in their outreach, these interventions come amongst countless other reports, court orders, debates have been circulating in the digital rights circuit that aim to fight the fight over spyware technology.

Despite these efforts, surveillance remains a booming, largely unregulated industry across the globe - especially in the developing world, where the effects are even further heightened with its impact on marginalized communities. Over 500 surveillance tech companies continue to market and sell these tools to around 65 governments worldwide, many of them located in the Global South, with no transparency mechanisms in place. Just over 5 years ago, Meta in collaboration with Citizen Lab detected a Pegasus spyware attack via WhatsApp chat messenger; a breach that affected users across the globe, with a significant concentration of targets in Mexico, Pakistan, India, Bahrain, and Morocco.[8] Similarly, the diverse Chinese surveillance economy has enabled neighbouring countries to acquire highly sophisticated technology with little to no international or national convention to hold them accountable for its use.

---

[6] Stephanie Kirchgassener, “USA: Israeli spyware company NSO Group placed on commerce department blacklist,” Business & Human Rights Center, November 3, 2021, https://www.business-humanrights.org/en/latest-news/usa-israeli-spyware-company-nso-group-placed-on-commerce-department-blacklist/

[7] “The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities,” gov.uk, February 28 2025, https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

[8] Lorenzo Franceschi-Bicchierai, “Court document reveals locations of thousands of WhatsApp victims targeted by NSO spyware,” Business & Human Rights Resource Centre, April 9 2025, https://www.business-humanrights.org/en/latest-news/court-document-reveals-locations-of-thousands-of-whatsapp-victims-targeted-by-nso-spyware/

In recent years, this surge has also been witnessed in South Asia, where a significant rise in sophisticated digital surveillance by both state and non-state actors has been used to target voices of dissent and controversy in the region. From massive data leaks across the region amidst rising biometric and digital identity programs to increasingly invasive intercepting technologies used on direct communication channels and internet monitoring attacks, governments have been investing chunks of their yearly budgets into acquiring technologies that allow them to track, record, and scrutinize the public without the public ever holding any knowledge around this for years. This diversity of technologies alongside the knowledge to manipulate them shows just how intricate the surveillance landscape is in South Asia, and it is only becoming more and more complicated.

With shoddy and ambiguous legal frameworks barely in place in South Asia, an international move towards digital integration with little concern for privacy oversight, and a mounting concern for "national security", cyber intrusion and surveillance have become faster, easier, and more invasive than ever before. Moreover, such poor governance, lax policies, and informal record keeping has given surveillance industry players, that largely operate out of the West, the opportunity to benefit from and profit off of unstable regimes. For example, European-owned surveillance company FirstWap was exposed late last year by Lighthouse Reports to be selling surveillance technologies through an intermediary company set up in East Asia (Indonesia) easily contravening sanctions and export controls imposed by the EU and other western regulatory bodies.[9] As this report will point out, this is just one of many such cases and while efforts to bring these overarching powers under formal and legalized control have been underway, they are largely restricted to actors in the Global North whose perspectives lack the nuance and realities of experiences and injustices unique to this region.

Through a series of scoping studies from South Asia, Digital Rights Foundation (DRF) has undertaken the task to fill the gap in existing works, offering a more comprehensive analysis of legal, technological and societal impacts of surveillance tech and their deployment by states. A year-long effort made in collaboration with local researchers and experts in human rights, technology, and surveillance in the region, this series offers a cross-country examination that looks at the surveillance architecture in South Asia, the acquisition of emerging technologies in surveillance and highlights the role of existing inadequate legislation in aiding this blanket watchfulness in South Asian states.

---

[9] Lighthouse Reports, 'Surveillance Secrets,' Lighthouse Reports, October 14 2025, https://www.lighthousereports.com/investigation/surveillance-secrets/

In this series, four South Asia countries - Pakistan, India, Bangladesh and Sri Lanka - examine the historical context of surveillance in their respective governments, the legal framework (or lack thereof) and oversight mechanisms available, and the technologies that have been leveraged in recent years to exploit these legal loopholes and shaped the surveillance infrastructure and practices in the region.

As these studies will show, such a vast arsenal of surveillance technology combined with limited legal safeguards in place, creates nothing short of an Orwellian state of affairs that work towards repressing society and political dissent. The objective is not only to inform and alert the public about the growing ecosystem of surveillance in South Asia and the dangerous precedents that are being set in South Asia by the deployment of these technologies. The study urges the public to take a closer look at the existing legal and governmental apparatus that covertly facilitate and hinder their personal lives to be collected, stored, and analysed through technology. The study asks civil society organizations, journalists and citizens to ask the uncomfortable, important questions and demand the answers they deserve. And it forces governments to come face to face with their own actions while calling on their policymakers to start a dialogue on safeguards, transparency and accountability.

Methodology

This study takes on the herculean task of analysing historical precedents from the colonial era to understand how surveillance laws have been shaped into the draconian frameworks that they are today, as well as untangling critical threads around spyware technology, where it is acquired from and how it is deployed across the region for state and non-state surveillance. Under the supervision of the Digital Rights Foundation, 4 research experts were contracted from each country to ensure an in-depth understanding of country-specific dynamics that are part and parcel of the surveillance landscape.

Each study delves into a comprehensive review of history, precedents, laws, deployment of recent surveillance tech and policies and how they're intertwined in a web of privacy rights, data protection, and surveillance. Beginning with a deep dive into the evolution of surveillance in their respective countries, the studies examine and uncover existing supply chains in the world of spyware technology that feed into an environment of supervision over citizens and their activities, especially when they involve speaking against the status quo. Additionally, they explain legislative frameworks, including ICT and telecom regulations that make up the foundation of this global surveillance infrastructure and its impact in South Asia.

To gain unique and lived insights along with operational practices, the researchers relied on secondary data available on the subject and conducted semi-structured interviews with a range of stakeholders such as activists, lawyers, journalists, as well as civil society representatives who work closely within the digital rights space. Considering the sensitive nature of these revelations and while adhering to ethical research practices, experts interviewed were explicitly asked for their verbal consent to have their views and opinions expressed in this study, with their names and credentials. Experts who wished to stay anonymous have been given pseudonyms where possible to protect their identities, given the security concerns attached to such a topic.

At the conclusion of the series, an index will be presented that ranks all four countries according to how safe or unsafe they are from surveillance. Based off of a three-point model that analyses the legal recourse in place, existing cyber intrusive apparatuses available and the larger socio-political context of the country's while also taking into account conversations with trusted partners and experts in the field, this index will help put into perspective exactly how vulnerable the region is to growing cyber intrusions.

Limitations

Several challenges have formed the scope of this research. Since South Asia has a notorious reputation for limiting public access to government documents that should be available for a just democratic and civic process, many researchers during the course of this study had difficulties securing access to official records, including public tenders for government spyware procurement, state contracts and licensing agreements. Even requests made under Right To Information (RTI) were either met with bureaucratic red tape, silence or, most commonly, rejection under the guise of “national security.” The scope of the study, therefore, is specific to public information available online, including news articles, case laws, research papers along with experiences shared by experts in the field.

Additionally, early on in the study, efforts were made to ensure accuracy and balance - specifically through carving out space for opinions from state officials. While many civil servants in information, communication and technology (ICT) departments along with policymakers were contacted multiple times and asked for comment to give their perspective on how the government justifies cyber intrusion against its citizens, mainly to quell discourse, all were unresponsive. The lack of a government standpoint is deeply felt in the studies and is attempted to be supplemented by government press releases, state addresses and speeches that might shed light on their actions.

PAKISTAN

Chapter 1

DRF USA

Abbreviations

ATA	Anti-Terrorism Act
COE	Common Operations Environment
DRF	Digital Rights Foundation
FBR	Federal Bureau of Revenue
FIA	Federal Investigation Agency
FIR	First Information Report
IB	Intelligence Bureau
ICCPR	International Covenant on Civil and Political Rights
IFTA	Investigation for Fair Trial Act
IHC	Islamabad High Court
IP	Internet Protocol
ISI	Inter-Services Intelligence

LHC	Lahore High Court
LIMS	Lawful Interception Management System
MoITT	Ministry of Information, Technology and Telecommunications
NADRA	National Database and Registration Authority
PECA	Pakistan Electronic Crimes Act
PPP	Pakistan People's Party
PSCA	Punjab Safe Cities Authority
PTA	Pakistan Telecommunication Authority
PTI	Pakistan Tehreek-e-Insaf
VPN	Virtual Private Network

Introduction

Over the years, Pakistan has developed a sophisticated state surveillance system that significantly outpaces its legal frameworks. The Pakistani government justifies this surveillance as necessary to counter internal and external threats, particularly towards armed militant groups and terrorism. However, these capabilities have often been misused, including spying on opposition politicians and Supreme Court judges. Despite occasional judicial attempts to establish boundaries, deliberately vague legislation, technological advancement, and international security partnerships have expanded state surveillance beyond effective oversight. The highly politicized use of these capabilities against political opponents, judges, and journalists — rather than exclusively for legitimate security threats — has created a governance environment with minimal accountability.

Historical Context

Pakistan's history of communications surveillance can be traced back to British colonial rule, when it primarily involved physical surveillance and monitoring carried out via agencies including the Special Branch, Criminal Investigation Agency, and Intelligence Bureau (IB).[1]

The first significant expansion occurred under Prime Minister Zulfikar Ali Bhutto, who established a specialized cell within the IB (called the "Mukhtar Force") in 1972 to monitor senior military officials. Bhutto was also the first to order the Inter-Services Intelligence (ISI) to tap phones of political opponents during protests in 1977 — making him the last civilian leader to exercise direct control over the ISI.[2]

Following General Zia's 1977 coup, military intelligence agencies gained expanded roles and capabilities through US technical assistance during the Soviet invasion of Afghanistan (1979) - – a decade-long fight against communism that brought in dollars, weapons, and the ideological expansion of the military as the political.[3]

By the 1990s, intelligence operations had become heavily politicized. While the military-controlled ISI targeted Pakistan People's Party (PPP) politicians, the civilian-controlled IB conducted counter-intelligence to minimize ISI's political influence. This period saw the infamous "Operation Midnight Jackal," where IB operatives recorded conversations about the army's efforts to remove Prime Minister Benazir Bhutto through a no-confidence vote.[4] This murky incident highlighted existing rivalries within intelligence agencies – but also raised the alarming possibility that individuals within these agencies may have been acting on their own, beyond the purview of the state.[5]

---

[1] Sher Ali Khan, 'The state bytes back: Internet surveillance in Pakistan,' DAWN, 23 May 2017, https://herald.dawn.com/news/1153312 (accessed on 1 September 2025)

[2] Ibid

[3] Maham Fazal, 'General Zia-ul-Haq's Dark Legacy: How One Man Rewired The Soul of Pakistan,' The Friday Times, 5 July 2025, https://www.thefridaytimes.com/05-Jul-2025/general-zia-ul-haq-s-dark-legacy-how-one-man-rewired-the-soul-of-pakistan (accessed on 1 December 2025)
Dilip Mukerjee, 'Zia's Military Legacy,' in The Round Table, 310, 15 April 2008, http://dx.doi.org/10.1080/00358538908453924 (accessed on 1 December 2025)

[4] Idrees Bakhtair & Zaffar Abbas, 'The mysterious case of Operation Midnight Jackal,' Herald, 19 November 2018, https://herald.dawn.com/news/1398719 (accessed on 1 September 2025)

[5] Ibid

Under Masood Sharif Khattak's leadership of the IB (1993-1996), the agency modernized with increased recruitment and new technology, including its first computers. However, controversy emerged when Khattak's IB was accused of widespread surveillance, tapping phones of Supreme Court justices, high court judges, and opposition politicians like Nawaz Sharif.

These allegations became central to a constitutional petition – Mohtarma Benazir Bhutto and Ors. vs. President of Pakistan and Ors. – regarding Benazir Bhutto's government dismissal. In November 1996, former Prime Minister Benazir Bhutto and Yousaf Raza Gilani filed a petition before the Supreme Court challenging the President of Pakistan's dissolution of the national assembly and removal of Bhutto as Prime Minister. While the court upheld the presidential order 6-1, it also established strict limitations on surveillance, declaring that phone-tapping "interferes with the right of free speech and expression" and linking "inviolability of privacy" with "dignity of man." The court mandated that future surveillance required prior Supreme Court permission. This decision established important precedents for privacy rights and judicial oversight of government surveillance in Pakistan.[6]

Concurrently, Pakistan's digital communications were developing independently through individuals like Amjad Farooq Alvi, who imported computer hardware and established early computer networks in the 1980s – and was also the mastermind behind the first ever computer virus, "Brain". Intelligence agencies eventually took interest in Alvi's technology, with officials approaching him to understand how telephones could transfer data, marking the beginning of digital surveillance capabilities. Similarly, the introduction of Pakistan's international dialing code (+92) enabled easier interception of calls through computerized systems rather than the previous manual methods.[7]

By the late nineties, a slew of laws further expanded the state's surveillance capabilities. The 1996 Pakistan Telecommunication (Re-Organisation) Act significantly expanded government surveillance powers, allowing authorities to intercept communications in the name of "national security" or for "apprehension of any offence" — terms criticized for their deliberate vagueness and flexible interpretation.

---

[6] Sahar Iqbal, 'The right to be forgotten in Pakistan,' International Bar Association, 22 August 2023, https://www.ibanet.org/the-right-to-be-forgotten-in-Pakistan (accessed on 1 September 2025)

[7] Privacy International, 'Tipping the scales: Security & surveillance in Pakistan,' July 2015, https://privacyinternational.org/sites/default/files/2018-02/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf (accessed on 1 September 2025)

In 1997, the Anti-Terrorism Act (ATA) further extended these powers, permitting law enforcement to search premises without warrants. Though the Lahore High Court (LHC) struck down parts of the ATA as unconstitutional, it upheld surveillance provisions as necessary for counterterrorism, a view later affirmed by the Supreme Court.

This unrestricted surveillance became public in 2001 when the Sunday Times published transcripts of phone conversations between Prime Minister Nawaz Sharif and Supreme court judges who had convicted Benazir Bhutto.[8] Attorney General Aziz A Munshi later confirmed that Sharif's government had tapped judges' phones and presented a 75-page list of monitored numbers including politicians, journalists, and government officials.[9]

Throughout the 2000s, Pakistan kept expanding its surveillance capabilities, with the ISI forming a cyber unit and acquiring monitoring equipment from China and North Korea.[10] Specifically, following 9/11, the US and UK provided technical assistance and modern equipment to Pakistani agencies while the US National Security Agency (NSA) established listening posts in Pakistan for joint surveillance operations targeting al-Qaeda and Taliban communications; a cooperation that largely ended after the 2011 Bin Laden raid.[11]

Pakistan authorities also ventured into mass surveillance space and their interest dates back to at least 2005, and has been facilitated by both domestic and foreign surveillance companies. In 2013, Pakistan's Inter-Services Intelligence (ISI) agency sought to build a mass surveillance system capable of tapping international undersea cables at three landing sites in southern Pakistan.[12]

---

[8] Irfan Husain, 'Rush to judgement,' DAWN, 10 February 2001, https://www.dawn.com/news/1072392 (accessed on 1 September 2025)

[9] Noor Ejaz Chaudhry, 'Big Brother: Mapping State Surveillance of Citizens Online and Offline,' Digital Rights Monitor, 8 February 2021, https://digitalrightsmonitor.pk/pakistan-as-big-brother-mapping-state-surveillance-of-citizens-online-and-offline/ (accessed on 1 September 2025)

[10] Abhishek Kumar, 'Revisiting the Nuclear Nexus between Pakistan, China, and North Korea,' Institute for Security and Development Policy, 5 January 2023, https://www.isdp.eu/revisiting-the-nuclear-nexus-between-pakistan-china-and-north-korea/ (accessed on 1 September 2025)

[11] Adnan Chaudhri, 'Spectrum Eyes: The NSA & Pakistani Metadata,' Digital Rights Foundation, 14 May 2015, https://digitalrightsfoundation.pk/spectrum-eyes-the-nsa-pakistani-metadata/ (accessed on 1 September 2025)

[12] Privacy International, 'Pakistan: Intelligence agency sought to tap all communication traffic, documents reveal,' Privacy International, 21 July 2015, https://privacyinternational.org/blog/1364/pakistan-intelligence-agency-sought-tap-all-communications-traffic-documents-reveal (accessed on 1 September 2025)

Additionally, they reportedly hired intermediary companies to acquire spying toolkits from western and Chinese firms such as FinFisher, SS8, and Utimaco, to carry out domestic surveillance – tapping all IP bound communications traffic entering or travelling through Pakistan. Reports published by Privacy International, The Guardian, as well as Dawn in 2015-17 stated that this Targeted IP Monitoring System and Common Operations Environments (COE) would collect approximately 660 gigabytes of data per second at a centralized command center, representing a significant expansion of Pakistan's communications intelligence gathering capacities.[13]

Furthermore, amid concerns around use of illegal SIMs during terror operations, since 2016 all SIM cards in Pakistan are required to be registered against their user, as well as verified – via fingerprint – against biometric data held by the National Database and Registration Authority (NADRA).[14] This implies that all citizens with access to SIMs are also susceptible to being tracked or targeted, or having their private information (such as phone numbers or National Identity Card numbers) misused.[15] There have also been major breaches of citizens' personal data held by the government: In 2021 local news reports revealed the NADRA's biometric database had been hacked, and that a number of "fake SIMs" had been exported.[16]

Interestingly, the web of intrusive technology was not limited to just Pakistani actors. Reportedly, in 2013, the NSA tapped fibre optic cables landing in Karachi, among others, and used 55 million phone records harvested from private Pakistani telecommunications providers for an analysis exercise.[17] Similarly, the UK's Government Communications Headquarters (GCHQ) had a store of "kis" key from Mobilink and Telenor mobile networks, two of the country's biggest telecom providers.[18]

---

[13] Sher Ali Khan, 'The state bytes back: Internet surveillance in Pakistan,' DAWN, 23 May 2017, https://herald.dawn.com/news/1153312 (accessed on 1 September 2025)

[14] Tim Craig & Shaiq Hussain, 'Pakistan's mobile phone owners told: be fingerprinted or lose your sim card,' The Guardian, 3 March 2015, https://www.theguardian.com/world/2015/mar/03/pakistan-fingerprint-mobile-phone-users (accessed on 1 September 2025)

[15] Privacy International, 'Timeline of SIM Card Registration Laws,' 11 June 2019, https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws (accessed on 1 September 2025)

[16] Javed Hussain, 'Nadra's biometric data has been compromised, FIA officials tells NA body,' DAWN, 25 November 2021, https://www.dawn.com/news/1660199 (accessed on 1 September 2025)

[17] Privacy International, 'Tipping the scales: Security & surveillance in Pakistan,' July 2015, https://privacyinternational.org/sites/default/files/2018-02/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf (accessed on 1 September 2025)

[18] Jeremy Scahill & Josh Begley, 'The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle,' The Intercept, 19 February 2015, https://theintercept.com/2015/02/19/great-sim-heist/ (accessed on 1 September 2025)

While the upgrades to surveillance/cyber intrusion infrastructure were understandably taken amid a domestic war on terror, the recent instances of audio leaks just as the opposition party Pakistan Tehreek-e-Insaf (PTI) has fallen out with the establishment is a stark reminder of how these technologies continue to be readily deployed against political dissidents.[19] News reports published in July 2024 revealed the existence of a "Lawful Intercept Management System" (LIMS) deployed by the Pakistan Telecommunications Authority (PTA)[20] - a development that has since been investigated by Amnesty International in their report on Pakistan's growing surveillance economy.[21] This news came to light following a court case filed last year by former Prime Minister Imran Khan's wife Bushra Bibi and Najam Saqib, son of former chief justice of Pakistan Saqib Nisar, against alleged audio leaks.[22] Further reports revealed that surveillance via LIMS extends to all communications carried out by consumers through the network of the telecom providers.

Digital rights experts and journalists have lobbied against the use of LIMS, stating that it is "unlawful" and "invasive", and that any form of surveillance carried out without a warrant is in violation of both, the Fair Trial Act 2013 and the Prevention of Electronics Crime Act (PECA) 2016. Nonetheless, the state continues to justify the use of invasive technology under the guise of "national security."[23]

---

[19] Rizwan Shehzad, 'High-powered panel to probe audio leaks,' The Express Tribune, 5 October 2022, https://tribune.com.pk/story/2380194/high-powered-panel-to-probe-audio-leaks (accessed on 1 September 2025)

[20] Zaki Abbas, 'The surveillance system keeping tabs on millions,' DAWN, 2 July 2024, https://www.dawn.com/news/1843299 (accessed on 1 September 2025)

[21] Amnesty International, 'Shadows of Control: Censorship and mass surveillance in Pakistan,' 9 September 2025, https://www.amnesty.org/en/documents/asa33/0206/2025/en/ (accessed on 9 September 2025)

[22] Umer Mehtab, 'Audio leaks case: IHC dismisses IB's petition to withdraw plea seeking Justice Sattar's recusal,' DAWN, 3 May 2024, https://www.dawn.com/news/1831190 (accessed on 1 September 2025)

[23] Rizwan Shehzad, 'Govt defends legal cover for surveillance,' The Express Tribune, 10 July 2024, https://tribune.com.pk/story/2478373/govt-defends-legal-cover-for-surveillance (accessed on 1 September 2025)

Findings

Prevalence of Cyber Intrusion

Pakistan's privacy and cybersecurity landscape is nebulous and unwieldy. Although the law – constitutionally – guarantees the right to privacy, intelligence agencies continue to usurp those rights by tapping phones and other means of communication used by politicians, human rights activists, journalists and government officials.

Reports released by Canada-based Citizen Lab in 2013 and the Digital Rights Foundation (DRF) in 2014 revealed the existence of two servers operated by surveillance company FinFisher in Pakistan. Further reports revealed that a Pakistani entity purchased three tools from FinFisher – FinSpy, FinUSB, and FinIntrusion Kit.[24] The tools enabled remote access to user devices, infection of USBs, and interception of Wi-Fi traffic, even in encrypted sessions. These capabilities raise significant concerns about privacy violations and unchecked surveillance.

These investigations – as well as prior technical confirmations by Citizen Lab – point towards the likely involvement of a Pakistani intelligence agency, as FinFisher claims to sell only to government clients.[25] The evidence included screenshots of license agreements, support chats with a Pakistani user identified as "Khalid", and use cases involving spyware embedded in PowerPoint files.

When human rights organization Bytes for All challenged these surveillance practices in 2014 and 2015 through legal action citing constitutional violations, court proceedings were repeatedly delayed without resolution, while government officials either declined to comment or professed ignorance about the technology's deployment.[26] These capabilities exist within the broader global context of mass surveillance systems similar to those revealed by Edward Snowden, leaving ordinary citizens with limited protection against state-level monitoring despite basic security precautions.

---

[24] Jahanzaib Haque, 'Customer 32 - who used FinFisherto spy in Pakistan?' DAWN, 24 August 2014, https://www.dawn.com/news/1127405 (accessed on 1 September 2025)

[25] Ibid

[26] Hasan Abdullah, 'Fishing in troubled waters,' DAWN, 26 April 2015, https://www.dawn.com/news/1177605/fishing-in-troubled-waters (accessed on 1 September 2025)

Human rights advocates warn that these tools pose a serious threat to journalists, activists, and other vulnerable groups, especially in a context where rigid privacy laws and regulatory oversight are absent. This also underscores an urgent need for transparency, regulation, and judicial scrutiny of state and military surveillance practices in Pakistan.

Pakistan operates a comprehensive mass surveillance infrastructure called LIMS, ordered and deployed by the PTA as far back as 2007. The system, made mandatory for all telecom companies as part of their licensing agreements for operations in the country, is financed and installed at designated "surveillance centers", which enables authorities to conduct warrantless interception of citizens' communications data.[27]

News about LIMS publicly surfaced after petitions were filed by former Prime Minister Imran Khan's wife Bushra, and others, in the Islamabad High Court (IHC), challenging the leaking of their telephonic conversations and subsequent unauthorized surveillance and privacy violations. According to court documents from the Islamabad High Court (IHC), obtained by Dawn, LIMS allows the PTA and other designated intelligence agencies to track any SIM, IMEI number, or MSISBN identity with "the click of a button" – capturing SMS messages, call data, metadata, and complete audio/video content without human intervention or judicial oversight. The court later observed that this mass surveillance system "lacked a legal foundation" and was being put in place without judicial or executive oversight.[28] The scale of surveillance carried out via LIMS is significant, with telecom licensees obligated to ensure up to 2% of their entire consumer base can be monitored simultaneously - approximately 4 million Pakistani citizens at any given time.

[27] Zaki Abbas, 'The surveillance system keeping tabs on millions,' DAWN, 2 July 2024, https://www.dawn.com/news/1843299 (accessed on 1 September 2025)

[28] Saima Shabbir, 'Rights activists raise privacy concerns after Pakistan authorizes top spy agency to tap calls, messages,' Arab News, 9 July 2024, https://www.arabnews.com/node/2546556/%7B%7B (accessed on 1 September 2025)

Pakistan has ventured into a new avenue of surveillance through its pursuance of a "national internet firewall" capable of sifting through internet traffic to help authorities continuously monitor and regulate online content especially on popular applications such as WhatsApp.[29] Initial reports made in July 2024 from across the country shared grievances of frequent internet slow downs and poor service quality from public and private ISPs alike. While at first the government posed changing narratives for why these internet disruptions were taking place, official confirmation was given (and retracted) in August by the Minister of Defence and Minister of MoITT about the installation of an upgraded Web Monitoring System (WMS), acquired from Chinese cyber intelligence firms.[30] First deployed in 2019, the WMS is posed as a tool for "content management," which utilizes the government to monitor all internet traffic entering or leaving the country's digital borders by employing deep packet inspection. Deep packet Inspection, also known as DPI, is a process of rummaging through internet traffic to examine incoming information packets to detect and/or prevent any incoming cyberattacks, among other uses.[31] Though largely used by organizations and ISPs to filter out any harmful or potentially dangerous information passing through their servers, its use by the state can quickly be manipulated to identify, analyze, locate, and block packets as needed. journalists and activists have expressed concern over its use by the state to effectively "surveil citizens' digital activity almost constantly."[32]

This watchful eye over what gets posted, shared, commented, and liked combined with the power to censor, block or delete disagreeable content creates a consistent environment of repression in Pakistan for all but especially for journalists, human right activists, and opposition members who speak up online against state injustices.

---

[29] Abid Hussain, 'Pakistan tests secret China-like 'firewall' to tighten online surveillance,' Al Jazeera, 26 November 2024, https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance (accessed on 1 September 2025)

[30] Nadir Guramani, 'NA informed Web Monitoring System deployed to block applications, websites not in agreement with law,' DAWN, 30 August 2024, https://www.dawn.com/news/1855782 (accessed on 1 September 2025)

[31] Integrated Research, 'Deep Packet Inspection (DPI): How it works and why it's important,' Integrated Research, https://www.ir.com/guides/deep-packet-inspection (accessed on 1 September 2025)

[32] Umer Ali & Ramsha Jahangir, 'Pakistan moves to install nationwide 'web monitoring system'' .Coda, 24 October 2019, https://www.codastory.com/authoritarian-tech/pakistan-nationwide-web-monitoring/ (accessed on 1 September 2025)

Most recently, the Finance Act 2025 – passed by the National Assembly of Pakistan in July 2025 – significantly undermines data privacy in Pakistan by granting tax commissioners sweeping powers to access subscriber information and IP address data from internet service providers and telecom companies without judicial oversight. The Act's phrasing – including the phrase "notwithstanding anything contained in any other law" – effectively overrides existing privacy protections, allowing direct administrative access to personal digital information including browsing histories, communication patterns, and online activities under the broad pretext of tax fraud investigations. It represents a concerning expansion of state surveillance capabilities that prioritizes administrative convenience over individual privacy rights, creating potential for abuse and overreach in a country where data protection frameworks are already inadequate and implementation of privacy safeguards remains weak.

The unregulated nature of this surveillance creates substantial risks for Pakistani citizens, particularly journalists, human rights defenders, and marginalized groups whose movements can be tracked online. Digital rights advocates have called for judicial and parliamentary oversight mechanisms, accountability for telecom companies that have "failed their consumers," and enforcement of privacy protections under Article 14 of Pakistan's Constitution. The absence of an adequate data protection law compounds these concerns, especially given past security breaches of government databases held by NADRA, the Federal Bureau of Revenue (FBR), and the Safe City systems.

And laws that have been presented, have drawn criticism from civil society and activist groups. In 2023, the Ministry of Information and Technology and Telecommunications (MoITT) circulated a draft of the Personal Data Protection Bill, 2023 with civil society and activist groups, from whom it received unanimously negative feedback, particularly regarding government demands for data localization.[33] Privacy International published a statement in which they stated that they were "concerned by developments in Pakistan regarding the enactment of the Draft Personal Data Protection Bill, 2023 and the opaque process which will see the bill become law."[34] The Asia Internet Coalition also raised similar concerns (Amin, 2023).[35]

---

[33] Cloudflare. 'Data localization is the practice of keeping data within the region it originated from.' Cloudflare. https://www.cloudflare.com/en-gb/learning/privacy/what-is-data-localization/ (accessed on 1 September 2025)

[34] Privacy International, 'Privacy International raises concerns regarding Pakistan's Personal Data Protection Bill,' Privacy International, 8 August 2023, https://privacyinternational.org/news-analysis/5090/privacy-international-raises-concerns-regarding-pakistans-personal-data (accessed on 1 September 2025)

[35] Tahir Amin, 'AIC raises questions about 'Pakistan Draft Data Protection Bill 2023',' Business Recorder, 24 July 2023, https://www.brecorder.com/news/40254218/aic-raises-questions-about-pakistan-draft-data-protection-bill-2023 (accessed on 1 September 2025)

In an op-ed for Dawn published in July 2023, digital rights activist Usama Khilji claimed that data localization requirements specified under the Personal Data Protection Bill 2023 would force companies to establish data centers in Pakistan and process critical personal data locally, while also mandating the sharing of sensitive personal data with the government.[36] Establishing local data centers helps to keep vital citizen information within the country and out of reach of foreign entities with burgeoning jurisdiction problems, the concern remains whether the Pakistani government themselves gain access and control of such information. Furthermore, the broad definitions of what constitutes critical and sensitive data may lead international companies to stop offering certain services due to high compliance costs, undermining the internet's purpose of facilitating communication and business.

[36] Usama Khilji, 'Silencing Pakistan,' DAWN, 28 July 2023, https://www.dawn.com/news/1767243 (accessed on 1 September 2025)

State Rationale

Based on expert interviews and case analysis, the deployment of cyber intrusion technologies in Pakistan is driven by multiple interconnected rationales that extend beyond stated security objectives of the government.

Shmyla Khan, a researcher and digital rights expert interviewed for this study attributed the state's continual use of "national security" as justification for deploying surveillance technology towards a "[colonial] hangover," – a constant state of unquestioning approval given towards funds that go into acquisition of technology used for national security. "You get a blank check," she added. "Nobody in parliament is checking. There is no oversight, and no accountability."

The national security justification becomes particularly powerful when considering the laundry list of laws that have been passed under its pretext: the Federal Investigation Agency Act, 1974; the Pakistan Telecommunication (Re-organisation) Act, 1996 and many other amendments to existing constitutional rights. The national security justification became particularly powerful after the 2014 Army Public School attack, which led to the National Action Plan and subsequently PECA, expanding surveillance powers of the state significantly.

Journalist Ramsha Jehangir notes that across multiple laws—the Pakistan Telecommunication Act, the Fair Trial Act, the FIA Act, and then PECA—there exists a consistent "language of access to citizen data for national security." This framing makes opposing such technologies politically difficult, as resistance can be characterized as undermining security interests.

Expert interviews reveal that a central unstated rationale for the deployment of surveillance mechanisms and cyber intrusive technologies – under the guise of national security – has created what digital rights activist Usama Khilji describes as "chilling effects" on political expression. The goal is ensuring "you know you're being watched...so inadvertently you end up self-censoring yourself," he added. This creates an environment where citizens, particularly journalists and activists, limit their speech out of fear.

Khan notes this political dimension became evident during the Prime Minister's Office audio leaks scandal in 2022, where "significant cybersecurity lapses" revealed sensitive political discussions, demonstrating how surveillance technologies meant for security can serve political purposes.[37]

The deployment of cyber surveillance technologies in Pakistan is notably fragmented across agencies. Khan observes: "The ways in which intrusive technology is deployed is also very disparate...there are multiple security agencies using it. The FIA has a different set of technologies, but the ISI might have something different."

This fragmentation serves two purposes: it creates redundancy in surveillance capabilities and makes oversight more difficult, as no single agency bears complete responsibility for surveillance activities.

Beyond passive monitoring, cyber intrusion tools enable active enforcement. Khilji notes that for journalists producing unwanted content, "you're going to be picked up, you're going to be put in handcuffs, you're going to be paraded around court." For diaspora critics, "this information is going to be used to find out who your family is, and then they're going to be harmed."

Recent years have seen several journalists and human rights activists in Pakistan surveilled by the state. A report published by the International Federation of Journalists in 2019 claims that several Pakistani journalists were placed on a ‘watch list’ by the Pakistan Federal Investigation Agency’s Cybercrime Wing over criticism of Saudi Crown Prince Mohammed Bin Salman during his visit to Pakistan in February 2019 (IFJ).[38] And in April 2025, a report published by Pakistani media and development sector watchdog Freedom Network documented a “worrying” trend of legal actions, arrests, enforced disappearances, censorship, attacks on journalists’ residences, and physical assaults – all levelled on the basis of Pakistan’s controversial cybercrime law.[39]

These tangible consequences, enabled by surveillance technologies, have created a powerful deterrent against political dissent in Pakistan.

---

[37] Abid Hussain, ‘Why is Pakistan investigating several audio leaks from PM office?’ Al Jazeera, 29 September 2022, https://www.aljazeera.com/news/2022/9/29/why-is-pakistan-investigating-several-audio-leaks-from-pm-office (accessed on 1 September 2025)

[38] International Federation of Journalists, ‘Pakistani government monitoring journalists’ social media activity,’ International Federation of Journalists, 1 April 2019, https://www.ifj.org/media-centre/news/detail/article/pakistani-government-monitoring-journalists-social-media-activity (accessed on 1 September 2025)

[39] Eesha Arshad Khan, ‘The Prevention of Electronic Crimes Act 2016: An Analysis,’ SAHSOL LUMS, https://sahsol.lums.edu.pk/node/12862 (accessed on 1 September 2025)

Major Breaches, Victims and Beneficiaries

In December 2017, Diep Saeeda, a Pakistani human rights defender, became the target of a sustained and highly personalized digital surveillance campaign after she began advocating for the release of peace activist Raza Khan, who was forcibly disappeared in that year.[40] Attackers posing as individuals – like “Sana Halimi” and “Mahrukh Zman” – used fake Facebook profiles to send her phishing links disguised as Facebook or Google login pages, malicious files labeled as documents about Raza, and Android spyware masked as mobile apps. The attackers also attempted to install custom-built malware such as Crimson on her devices, often using emotional manipulation and crafted pretexts associated with her activism.[41]

An investigation carried out by Amnesty International in 2018 revealed that these attacks were part of a broader campaign targeting human rights defenders in Pakistan, using a combination of social engineering, spearphishing, and surveillance tools. The malware used, including Crimson and StealthAgent, was traced to infrastructure and individuals based in Lahore, suggesting a deliberate and technically sophisticated effort to monitor and suppress civil society. These attacks not only threatened Saeeda’s personal security but also had a chilling effect on broader activism in Pakistan, reinforcing a climate of fear and surveillance that undermines the ability of human rights defenders to work safely and effectively.

These targeted attacks against civil society activists represent just one facet of Pakistan's broader cybersecurity challenges. Several subsequent events have further highlighted significant cybersecurity weaknesses in Pakistan's government systems. On August 14, 2021, Pakistan's FBR suffered a major cyberattack that disabled all its official websites for over 72 hours. As the national center for tax collection and documentation, this breach had serious security and financial implications. The attack occurred despite Pakistan's ongoing digital modernization efforts supported by the World Bank to upgrade what it called "end-of-life equipment" and "legacy branded software."[42]

---

[40] Amnesty International, ‘Pakistan: Campaign of hacking, spyware and surveillance targets human rights defenders,’ Amnesty International, 15 May 2018, https://www.amnesty.org/en/latest/news/2018/05/pakistan-campaign-of-hacking-spyware-and-surveillance-targets-human-rights-defenders/ (accessed on 1 September 2025)

[41] Ibid

[42] Shahbaz Rana, ‘ Neglect caused FBR cyber-attack,’ The Express Tribune, 22 August 2021, https://tribune.com.pk/story/2316604/neglect-caused-fbr-cyber-attack (accessed on 1 September 2025)

The FBR attempted to downplay the incident, terming it as "unforeseen anomalies during the migration process." While officials claimed they responded quickly and restored systems, uncertainty remains about whether core databases were compromised. The exact method of intrusion also remains unclear – some reports suggest hackers obtained administrator login credentials, while others point to a Hyper-V link vulnerability. More troubling, intelligence services reportedly warned of an impending cyberattack, raising critical questions about preparedness and response protocols despite significant investments in cybersecurity.

The FBR incident exemplifies Pakistan's digital security challenges that have emerged in recent years, where even sophisticated systems remain vulnerable. Pakistan ranks poorly in the Global Cybersecurity Index coming in at 94th and 18th place in global and Asia Pacific rankings respectively whilst trailing behind regional neighbors like Bangladesh, Sri Lanka, and India. Numerous Pakistani organizations have suffered cyber intrusions in recent years, including NADRA, various banks, and government institutions. The breaches targeting NADRA are particularly concerning given that the organization maintains the comprehensive database of all Pakistani citizens, containing sensitive personal information including biometric data, addresses, family relationships, and national identification numbers. Any compromise of NADRA's systems potentially exposes the entire population's personal data to malicious actors, creating risks for identity theft, fraud, and surveillance that could affect millions of citizens.

While Pakistan has taken some steps to address these issues, including enacting the PECA in 2016 and developing a cyber security policy in 2021, implementation remains inadequate. Furthermore, critics argue that laws like PECA have expanded state surveillance capabilities and granted excessive powers to authorities, potentially undermining civil liberties rather than enhancing genuine cybersecurity protections.

The FBR breach quickly transformed from a technical matter into one with significant political implications. With the government promoting electronic voting machines for elections involving millions of voters back in 2021, opposition parties cited the FBR breach as evidence of potential vulnerabilities in the electoral system.

The vulnerability of voter data has been compounded by the absence of a data protection bill for bodies like the Election Commission of Pakistan. This gulf was further highlighted in the 2024 elections, when political parties were able to access extensive voter lists beyond their constituencies for targeted advertisements and automated calls, raising ethical concerns about transparency, voter privacy, and fair electoral competition in an environment where weak data protection laws and inadequate implementation of regulations have exacerbated these problems.[43]

In October 2022, multiple audio leaks from Prime Minister Shahbaz Sharif's Office revealed sensitive conversations between top officials, including both current Prime Minister Shahbaz Sharif and former Prime Minister Imran Khan discussing official matters with their close aides and ministers. These leaks, reportedly part of a 140-hour collection of recordings offered for sale on the dark web for $3.45 million, caused considerable embarrassment and raised serious security concerns.

Former Prime Minister Khan condemned these leaks as "a serious breach of national security" and sought a judicial investigation, claiming he was planning on pursuing legal action to verify the authenticity of the recordings and establish which intelligence agency might be responsible for the surveillance. Prime Minister Sharif described this as "a very significant cyber security lapse" and established a high-level committee led by the interior minister to investigate.

The leaked audio contained politically sensitive content. Prime Minister Sharif was reportedly heard discussing importing industrial machinery from India for a relative, while his niece Maryam Nawaz allegedly requested the cancellation of a public health project initiated by Khan. Another recording appeared to capture Khan instructing his chief bureaucrat to "play up" a diplomatic cable from Pakistan's ambassador to the US without specifically naming the US.

---

[43] Digital Rights Foundation, 'Voter data privacy in Pakistan: Privacy risks, data protection, and legislative shortcomings during data-driven elections,' Digital Rights Foundation, January 2025, https://digitalrightsfoundation.pk/wp-content/uploads/2025/01/Voter-Data-Privacy-in-Pakistan.pdf (accessed on 1 September 2025)

These incidents have damaged Pakistan's diplomatic credibility, as foreign dignitaries may now hesitate to speak freely at the Prime Minister's House. Intelligence agencies were apparently unaware of the surveillance for months, though reports suggest the IB had recently warned the Prime Minister about the breach.

Judicial intervention – purportedly to bar intelligence agencies from directing telecom companies to surveil citizens – has also proven to be ineffective (Mohamand, 2024).[44] Specifically: In May 2023, Najam Saqib, son of former chief justice Saqib Nisar, filed a petition against a parliamentary inquiry into his alleged audio seeking bribes. This was later combined with a September petition by Bushra Bibi, former Prime Minister Imran Khan's wife, who challenged an FIA inquiry based on her leaked conversation with Khan's aide Zulfi Bukhari about selling Toshakhana gifts. The court responded by ordering intelligence agencies and the PTA to trace the sources of these audio leaks.[45]

In May 2024, the Islamabad High Court's Justice Babar Sattar barred the "federal government, intelligence agency or police" from exercising further surveillance, stating that "no entity or agency of the country has been authorised to undertake surveillance or undertake legal interception of telephone calls or telecom data" – and that doing so would be in violation the Telegraph Act, the Telecommunication Act, the Fair Trial Act and PECA.[46] This decision was later overturned by the Supreme Court of Pakistan in August 2024 (Momand, 2024).[47]

Pakistan's cybersecurity challenges represent a growing national security concern requiring comprehensive reforms in governance, technology infrastructure, and policy implementation. The series of breaches from 2021 to 2022 demonstrate that without significant improvements, the country remains vulnerable to both domestic and international cyber threats with serious implications for governance, diplomacy, and citizen privacy.

---

[44] Abdullah Momand, 'SC suspends IHC order in audio leaks case, bars court from further proceedings,' DAWN, 19 August 2024, https://www.dawn.com/news/1853303 (accessed on 1 September 2025)

[45] Umer Mehtab, 'Audio leaks case: IHC dismisses IB's petition to withdraw plea seeking Justice Sattar's recusal,' DAWN, 3 May 2024, https://www.dawn.com/news/1831190 (accessed on 1 September 2025)

[46] Umer Mehtab, 'IHC says those involved in and aiding surveillance of citizens are 'liable for offenses'' DAWN, 30 May 2024, https://www.dawn.com/news/1836404 (accessed on 1 September 2025)

[47] Abdullah Momand, 'SC suspends IHC order in audio leaks case, bars court from further proceedings,' DAWN, 19 August 2024, https://www.dawn.com/news/1853303 (accessed on 1 September 2025)

According to Jehangir, the journalist, primary beneficiaries of cyber surveillance technologies in Pakistan are security agencies and "whoever has control over the national security narrative." Indeed, existing state institutions have increasingly empowered themselves to use this concept to silence dissent and control the political process making it an increasingly monopolized conception of state security defined to fit the needs of the government rather than the people.

Conversely, victims of these technologies are not uniformly affected across Pakistani society. Jehangir notes that "citizens, but...definitely gendered minorities are definitely very much impacted," citing the Safe City project – a Karachi-based monitoring project involving installing numerous cameras and other surveillance equipment across the city – as an example where women's privacy is particularly compromised.[48]

A report compiled by DRF further elucidates that the Punjab Safe Cities Authority (PSCA) reveals a significant disconnect between state-imposed definitions of safety and citizen expectations. Through focus groups conducted in May 2023, DRF found that women's rights activists envisioned safe cities as physically secure and architecturally welcoming spaces for women and non-binary individuals, while lawyers and digital rights activists emphasized freedom from arbitrary law enforcement roadblocks and over-policing. The Punjab Safe Cities Project, – completed in January 2018 at a cost of twelve billion rupees – installed 8,000 CCTV cameras throughout Lahore with the stated aim of modernizing policing through digitization and eliminating "thana culture."

However, this analysis categorizes the project primarily as a policing modernization effort rather than genuine urban planning, finding that the Authority suffers from the same lack of accountability and transparency it claims to address, with officials refusing interviews on secrecy grounds and operating without legislative mandate or data protection policies. While the system has proven effective for monitoring large-scale events and holidays, DRF concluded that it failed to address everyday crime or reduce harassment of women in public spaces, and widened the scope of state surveillance.

[48] Tahir Siddiqui, 'Real-time surveillance begins under Karachi Safe City project, CM told,' DAWN, 20 November 2024, https://www.dawn.com/news/1873508 (accessed on 1 September 2025)

External Actors in the Mix

External actors have further complicated this already tenuous landscape. Recent investigations – by the BlackBerry Research and Intelligence Team and Sangfor Technologies – have uncovered that a sophisticated hacking group known as "SideWinder" has been conducting targeted cyber operations against the Pakistani government organizations since November 2022 (although cyber-attacks attributed to alleged external actors date back to at least 2018). This group, active since as early as 2012, focuses primarily on countries in Southeast Asia, with Pakistan being a frequent target alongside Afghanistan, Bhutan, China, Myanmar, Nepal, and Sri Lanka. Many cybersecurity experts believe SideWinder may be sponsored by the Indian government, though definitive attribution remains challenging in the cyber realm.

According to a report published by Kaspersky's SecureList, SideWinder is a highly sophisticated Advanced Persistent Threat (APT) group that demonstrates exceptional technical agility, capable of generating new malware variants within five hours of detection by security solutions (Dedola and Berdnikov, 2025).[49] For example, the group employs a multi-stage infection chain using spear-phishing emails that exploit CVE-2017-11882 to deploy custom tools including their "Backdoor Loader" and "StealerBot" espionage implant, with advanced anti-analysis techniques and Control Flow Flattening for evasion. Operationally, SideWinder conducts extensive target research to create personalized attacks tailored to specific victims, maintains persistent access on compromised networks, and has expanded their geographic reach across over 20 countries in South and Southeast Asia, the Middle East, and Africa. Their strategic capabilities include targeting diverse sectors from military and government entities to maritime infrastructure, logistics companies, nuclear energy facilities, and diplomatic missions, making them a persistent and dangerous threat to critical national infrastructure and sensitive government assets across multiple regions.

[49] Giampaolo Dedola & Vasily Bernikov, 'SideWinder targets the maritime and nuclear sectors with an updated toolset,' Securelist, 10 March 2025, https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/ (accessed on 1 September 2025)

SideWinder's attack methodology is of particular concern to security professionals because of its subtlety and effectiveness. The group typically begins by sending carefully crafted emails that appear legitimate to government employees. These emails contain attachments that, when opened, secretly install malware onto the victim's computer system. This malware creates what security experts call a "backdoor" – essentially a hidden access point that allows the hackers to return later and access the compromised system at will, potentially extracting sensitive information or causing disruption.

What sets these recent attacks apart is SideWinder's use of advanced evasion techniques.[50] The group has implemented a system called "server-based polymorphism" that helps them avoid detection by traditional security tools. When someone tries to access their malicious files, the system checks if the request is coming from a Pakistani IP address. If it is, the server delivers the dangerous version of the file; if not, it delivers a harmless version. This technique makes it extremely difficult for antivirus programs to identify the threat, as the malicious code essentially hides when being inspected by security systems. One specific target in this campaign was the Pakistan Navy War College, suggesting the attackers may be interested in military intelligence.

The scope of SideWinder's operations appears to be expanding. Recent findings by BlackBerry's cybersecurity researchers indicate that Turkey has also become a target of the group's intelligence collection efforts.[51] Additionally, SideWinder has diversified their attack vectors beyond email attachments, creating fake Android applications including cleaners and VPNs that were successfully uploaded to the Google Play Store. These seemingly legitimate apps were designed to harvest sensitive information from users' mobile devices, further demonstrating the group's technical sophistication and adaptability.

---

[50] BlackBerry, 'SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials - and Is Now Targeting Turkey,' Blackberry, 8 May 2023, https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan (accessed on 1 September 2025)

[51] Blackberry, 'Global Threat Intelligence Report,' BlackBerry, August 2023, https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/bbcomv4/blackberry-com/en/solutions/threat-intelligence/2023/threat-intelligence-report-august/Blackberry-Global-Threat-Intelligence-Report-August-2023.pdf (accessed on 1 September 2025)

At the same time, the Pakistani government also claims to have engaged in retaliatory cyberstrikes. During the May 2025 military conflict between Pakistan and India, both countries claimed to have engaged in extensive cyber warfare operations targeting each other's critical infrastructure. Both sides claimed significant success in their respective cyber operations, with Pakistani sources reporting access to over 90 government and corporate websites including those of the Indian Air Force and Border Security Force, while Indian reports highlighted the defacement of Pakistani government websites and attempted data theft from sensitive defense programs, illustrating how cyber warfare has become an integral component of modern military conflicts between the two nuclear-armed neighbors.

As of late, Pakistan has been found to be harbouring (and deploying) cyber-surveillance technology from Intellexa, a cybersecurity consortium infamous for its Predator software – a software that infects devices through malicious links that once opened, allows users to access encrypted messages, audio recordings, emails, location, photos, as well as the ability to activate the device's microphone.[52] A cyber intelligence investigation report published by Amnesty Security Lab in late 2025 shows how the highly intrusive software has, in the past months, been linked to various human rights abuses in the Global South, including the first recorded incident in Pakistan. In the summer of 2025, a human rights lawyer from Balochistan province was targeted by Predator's '1-click attacks' via WhatsApp from an unknown number and subsequently made vulnerable to surveillance and tracking. The attack, which relies on victims clicking a malicious link at least once to autodownload Predator's software in devices can give sweeping access to personal data as well as remote control of said device.

With this coming at a time when the province is undergoing massive civil unrest in the face of state restrictions, including internet shutdowns, it shows how cyber surveillance technologies can be used to exploit existing instabilities in regions across the world to by both buyers and sellers – for gaining illegal access to sensitive information that benefits an actor or to increase profits made from offering to target vulnerable communities.

[52] Amnesty International, 'To Catch a Predator: Leak exposes the internal operations of Intellexa's mercenary software,' Amnesty International, 1 December 2025, https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed/ (accessed on 5 December 2025)

Legal Framework

Privacy and Surveillance in the Law

Constitutionally, Pakistani citizens are guaranteed the right to privacy and dignity under the country's constitution, specifically, under Article 14 which states that "the dignity of man and, subject to law, the privacy of home, shall be inviolable." And yet, as this section will attempt to unravel, there have been several instances where citizens' right to privacy in Pakistan has had limits – especially when it comes to digital spaces. In other words, the Constitution protects the privacy of citizens, but that protection isn't unlimited – especially when it comes to things like online data and digital activities.

The legal foundation for electronic surveillance in Pakistan has evolved significantly over time, beginning with the Telegraph Act of 1885 imposed by the British government in India, which first established government powers to intercept civilian communications for public safety or emergencies. This early framework was later expanded through the Federal Investigation Agency Act of 1974, which created broader investigative powers for detecting various crimes. As telecommunications technology advanced, the Pakistan Telecommunication (Re-organization) Act of 1996 established a more comprehensive interception framework, granting the federal government authority to trace and intercept calls and messages under national security provisions.[53]

More recent legislation has attempted to address the growing complexity of digital surveillance. The Investigation for Fair Trial Act of 2013 represents the first detailed attempt to regulate electronic surveillance techniques such as wiretapping and communication interception, while PECA specifically addresses digital rights and access to electronic data (NACTA). These laws have progressively expanded the government's surveillance capabilities while attempting to establish legal boundaries for such activities.

[53] Pakistan Telecommunication Authority, 'Pakistan Telecommunication (Re-Organization) Act, 1996,' PTA, https://www.pta.gov.pk/assets/media/pta_act_consolidated_footnotes_11012022.pdf (accessed on 1 September 2025)

The regulatory framework has continued to evolve through additional measures that further define the scope of surveillance powers. The Monitoring and Reconciliation of Telephony Traffic Regulations of 2010 established detailed protocols for telecommunications monitoring and data retention requirements for service providers. Subsequently, various amendments to both PECA and the Investigation for Fair Trial Act (IFTA) 2013 have progressively expanded surveillance authorities, often in response to emerging security concerns and technological developments. The proposed Digital Nation Pakistan Bill represents the latest attempt to create a comprehensive digital governance framework, though its implications for privacy rights remain a subject of ongoing debate. This layered legislative approach has created a complex legal landscape where privacy protections exist alongside increasingly sophisticated surveillance mechanisms, often leading to tensions between individual rights and state security imperatives.

The rationale for deployment of these technologies also has deep historical roots. Ramsha Jehangir identifies "colonial thinking" as fundamental to Pakistan's approach, noting that "a lot of the laws we've inherited go back to British rule" and embody "a colonial way of controlling." This historical continuity suggests cyber intrusion technologies represent modern tools serving long-established control objectives. As Jehangir explains, this legacy creates a persistent power dynamic where authorities maintain "that frame of mind, like we are superior, we control the citizens...we get to decide who gets those protections."

Legal expert Mirza Moiz Baig notes, however, that there remains "a lack of regulation" particularly regarding the legal mandate of intelligence agencies deploying cyber intrusive technologies. "The problem with cyber intrusive technologies is that... there's an area where these agencies operate which is completely beyond the ambit [of the law]," Baig explains, highlighting a fundamental gap in Pakistan's legal surveillance framework.

Paradoxically, while Pakistan enacts surveillance capabilities on its citizens, the country has also ratified various international instruments to safeguard the privacy of citizens. These include the Universal Declaration on Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), the Convention on the Rights of the Child (Article 16), and the Cairo Declaration on Human Rights in Islam (Article 18). Consequently, the state is legally obligated to safeguard personal privacy as a basic human right through various legal frameworks that establish both protective measures and government responsibilities.

Despite these constitutional guarantees and international commitments, Pakistan continues to face significant challenges in addressing cyber intrusions and implementing comprehensive data protection legislation, creating a disconnect between the theoretical rights of citizens, surveillance enacted by the state, and the practical safeguards necessary to protect their digital privacy in an increasingly interconnected world.

Case Laws and Legal Precedents

Mohtarma Benazir Bhutto vs President Pakistan

To reiterate, the Constitution of Pakistan enshrines the right to privacy as a fundamental right under Article 14. Moreover, Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which Pakistan is a signatory, states that “no one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence.”

The scope and interpretation of Article 14 was brought into discussion by the Supreme Court in the case of Mohtarma Benazir Bhutto v President Pakistan (PLD 1998 SC 388).[54] This case represents one of Pakistan's most significant judicial decisions regarding privacy rights and has played a major role in shaping the understanding of privacy protections under Pakistan's constitutional framework.

Bhutto, who served twice as Pakistan's Prime Minister (1988-1990 and 1993-1996), brought this case before the Supreme Court in order to challenge government surveillance activities directed against her, specifically: alleged phone tapping and monitoring of her communications while she was out of office. In her constitutional petition, Bhutto argued that these surveillance actions violated her fundamental right to privacy guaranteed under Article 14 of Pakistan's Constitution.

[54] Noor Ejaz Chaudhry, ‘Big Brother: Mapping State Surveillance of Citizens Online and Offline,’ Digital Rights Monitor, 8 February 2021, https://digitalrightsmonitor.pk/pakistan-as-big-brother-mapping-state-surveillance-of-citizens-online-and-offline/ (accessed on 1 September 2025)

The government defended its position by citing national security concerns and referencing various laws permitting surveillance under certain circumstances. The Supreme Court's ruling on this case proved groundbreaking: it established that constitutional privacy protections extend beyond physical spaces to include communications privacy, and acknowledged that these rights, though fundamental, are not absolute and can be limited "subject to law" as stated in the Constitution.

This 1998 decision established crucial precedents for privacy rights in Pakistan by confirming that privacy protections apply to telecommunications, creating a judicial test for evaluating surveillance legality, and highlighting the ongoing tension between those who exert national security and the individual rights of citizens. Significantly, the Court determined that any form of government surveillance requires proper legal authorization through established procedures and cannot be conducted purely for political purposes or to monitor opposition figures without legitimate security justifications.

Constitutional law expert Umer Gilani confirms the significance of this ruling: "Article 14 of the Constitution specifically talks about the privacy of home being inviolable... [and in] Benazir Bhutto's case [the court] said that phone conversations are also covered by the guarantee regarding privacy of home, because your telecommunication is also part of the 'home'."

M.D. Tahir vs State Bank of Pakistan

Another notable precedent in privacy jurisprudence, as highlighted by Gilani, is M.D. Tahir v State Bank of Pakistan case from 2004. In this case, the FBR had instructed banks to routinely report account holders' annual income information without appropriate legislative authorization. The Lahore High Court struck down this practice in a public interest litigation, ruling that "bank account data is also your private data and the principle of data privacy applies," as Gilani explained. This established that financial information also falls under constitutional privacy protections and cannot be disclosed without proper legal provisions.

More recently, legal expert Mirza Moiz Baig points out how privacy concerns have reached the highest levels of Pakistan's judiciary. During the Justice Qazi Faez Isa case – a case in which former Chief Justice of Pakistan, Justice Isa, was accused of not disclosing information about foreign properties owned by his family members in his wealth statement – concerns emerged that "the Chief Justice Pakistan and his family were also being subjected to certain intrusive technologies." However, despite the Supreme Court acknowledging these concerns, even noting that "there was a government that went home just because of these allegations," Baig observes, as "Supreme Court proceedings aren't fact-finding proceedings... the Supreme Court did not eventually delve into that." This further illustrates the challenges of addressing surveillance through judicial remedies alone.

Audio Leaks Case

Furthermore, the Islamabad High Court's judgement on the audio leaks case – concerning alleged surveillance carried out on former Prime Minister Imran Khan's wife Bushra Bibi, and Najam Saqib, the son of former chief justice of Pakistan Saqib Nisar – in May 2024 also set an important precedent, barring telecom companies from recording phone calls and data for surveillance purposes. Digital rights activist Usama Khilji described the audio leaks case as a "watershed moment." "We saw the kind of strategies that the government has been using, or the state has been using [to enact surveillance]," he added. Two months after the judgement was passed, it was suspended by the Supreme Court, under a ruling which claimed that the "IHC's orders of May 29 and June 25 are beyond its authority."[55]

The principles established in these cases continue to influence how Pakistani courts interpret privacy rights in relation to newer legislations such as PECA, modern electronic surveillance activities and cyber intrusion, highlighting the persistent tension between constitutional privacy protections and the expansive surveillance powers granted to the state through various legislative acts. This judicial framework also helps contextualize contemporary debates about digital privacy in Pakistan, and provides us with a lens and useful roadmap for evaluating the constitutionality of surveillance and cyber intrusion.

[55] Abdullah Momand, 'SC suspends IHC order in audio leaks case, bars court from further proceedings,' DAWN, 19 August 2024, https://www.dawn.com/news/1853303 (accessed on 1 September 2025)

The Move Towards Codifying Cybercrime

PECA became law in August 2016 — despite widespread opposition from human rights defenders.[56] Those who opposed it said that the law was “ensnaring” innocent citizens, who were “unaware of the ramifications of what the bill entails” and that there were no provisions set in place “to protect sensitive data of Pakistani users.” (Reuters, 2016) This law emerged at a critical moment when Pakistan—a country with limited digital literacy —required thoughtful cybercrime legislation that would work within constitutional boundaries. Instead, citizens received a law allowing "authorised officers" to demand anyone unlock any device during investigations, regardless of privacy concerns.

The origins of PECA are directly tied to national trauma. Following the December 2014 Army Public School attack that claimed over 141 lives (of mostly children), Pakistan developed the 12-point National Action Plan as an urgent counter-terrorism response. Government officials repeatedly emphasized their need for "unfettered ability" to monitor and prosecute suspected militant activity, creating the perfect conditions for PECA's draconian provisions.

Legal expert Mirza Moiz Baig confirms this pattern of using national security to justify restrictive legislation: "Between 2012-2015, a lot of people spoke about how, for example, non-state actors, or how extremist organizations are using the internet, social media to their advantage... Then in 2016 we had PECA... introduced." He acknowledges that "there can be critiques about whether or not PECA offended fundamental rights itself, and perhaps it does," highlighting the tension between legitimate security concerns and civil liberties.

Though marketed as necessary to check extremist content, prosecute hate speech, and curb online harassment, PECA represented a significant departure from earlier cybercrime laws by moving beyond computer-related offenses to actively criminalizing speech and granting authorities unprecedented powers of surveillance. This pattern mirrors post-9/11 legislation in the United States (the Patriot Act) and United Kingdom (Anti-Terrorism, Crime and Security Act), both criticized for sacrificing civil liberties in the name of security.[57]

---

[56] Library of Congress, ‘Pakistan: National Assembly Passes New Cybercrime Law,’ Library of Congress, 21 September 2016, https://www.loc.gov/item/global-legal-monitor/2016-09-21/pakistan-national-assembly-passes-new-cybercrime-law/ (accessed on 1 September 2025)

[57] Farieha Aziz, ‘Pakistan’s Cybercrime Law: boon or bane?’ Heinrich Boll Siftung, 14 February 2018, https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane (accessed on 1 September 2025)

PECA's surveillance framework becomes particularly concerning bearing in mind the number of civilian arrests that have been carried out using its clauses as justification – particularly Section 20, which concerns “online defamation”, and the Pakistan Army (Amendment) Act, 2023, which states that anyone committing an offence under PECA or “any other relevant electronic, digital and social media laws” to “undermine, ridicule or scandalize the armed forces of Pakistan” triable. Apart from criminalization of online speech, journalists and human rights defenders in Pakistan are also directly impacted by the ways in which the law creates allowances for internet censorship, the takedown and interception of content, frequent – and often arbitrary – internet shutdowns, and the acquisition of data and seizure of electronic devices.[58]

In light of Pakistan’s lack of comprehensive data protection legislation, PECA becomes even more concerning: while the Electronic Transactions Ordinance 2002 and Freedom of Information Ordinance 2002 theoretically addressed data privacy, PECA fundamentally altered this approach. Rather than protecting citizens from data intrusion, its provisions primarily enhance government access to private information while restricting citizen access to government data, creating an asymmetrical system favoring state power over individual privacy.

The law's surveillance architecture operates through several troubling provisions. Section 31 allows law enforcement to demand personal data – ranging from devices such as cellphones, to call logs – without court warrants based solely on an officer's belief that information is "reasonably required" for investigations, with mere post-facto court notification. In vaguely defined "cyberterrorism" cases, officers can search, seize, and retain data without any prior judicial oversight.

Journalists and human rights defenders have also routinely been arrested under the provisions of this law, and their devices confiscated. Asad Ali Toor, a Pakistani journalist, was arrested on February 26, 2024, after appearing for questioning at the FIA’s cybercrime wing in relation to an alleged anti-judiciary campaign.[59]

---

[58] Digital Rights Foundation, ‘Voter Data Privacy in Pakistan: Privacy Risks, Data Protection, and Legislative Shortcomings During Data-Driven Elections,’ Digital Rights Foundation, January 2025, https://digitalrightsfoundation.pk/wp-content/uploads/2025/01/Voter-Data-Privacy-in-Pakistan.pdf (accessed on 1 September 2025)

[59] Committee to Protect Journalists, ‘Pakistan court remands journalists Asad Ali Toor in cybercrime case,’ Committee to Protect Journalists, 15 March 2024, https://cpj.org/2024/03/pakistan-court-remands-journalist-asad-ali-toor-in-cybercrime-case/ (accessed on 1 September 2025)

The FIA's First Information Report (FIR) accused him of launching an “anti-state” campaign through his YouTube channel Asad Toor Uncensored and his X (formerly Twitter) account, targeting civil servants, government officials, and state institutions in violation of the PECA. Three days before his arrest, FIA officials raided his Islamabad home, seizing his mobile phone and a portable internet device. He was held in FIA custody for 11 days before a court sent him to jail on a 14-day judicial remand pending investigation.

Section 32 of PECA compels Internet Service Providers to store user traffic data for at least one year (extended from 90 days in earlier drafts) and provide it to authorities upon request—a requirement that violates international privacy standards and has been struck down in jurisdictions like the UK for constituting disproportionate privacy interference. Government requests to Facebook for Pakistani user data increased from 719 in 2016 to over 1,050 in just the first half of 2017, with no transparency regarding justifications or usage.[60] Government requests to Google for content removal have also been on the rise, with over 450 filed in 2024.[61] In June 2024, the judicial magistrate court in Islamabad ordered the blocking of over two dozen YouTube channels – including those of former Prime Minister Imran Khan and critical journalists – for allegedly sharing “anti-state” content, following a report by the National Cyber Crime Investigation Agency. YouTube notified creators their channels could be removed under local law. The government also threatened criminal charges against content creators. Rights groups condemned the move as a crackdown on dissent, warning it conflates criticism with criminality. This comes amid broader efforts to control digital spaces, including amendments to Pakistan’s cybercrime law enabling harsh penalties and the creation of a new regulatory authority with powers to investigate and prosecute “false” online content.

Perhaps most concerning is Section 42's international surveillance cooperation framework, which grants the government virtually unlimited power to share citizens' data with foreign countries and agencies without judicial oversight or meaningful restrictions. This poorly drafted provision establishes no safeguards against potential misuse of sensitive personal data by foreign entities, revealing Pakistan's underdeveloped approach to information sharing.

---

[60] Asad Baig, ‘2900% increase in Pakistan government’s requests for Facebook ‘user data’ in last 5 years,’ Digital Rights Monitor, 21 December 2017, https://digitalrightsmonitor.pk/2900-increase-in-pakistan-governments-requests-for-facebook-user-data-in-last-5-years/ (accessed on 1 September 2025)

[61] Google, ‘Government requests to remove content,’ Google, https://transparencyreport.google.com/government-removals/government-requests/PK (accessed on 1 September 2025)

Current State Capacity and Response

Despite the extensive surveillance powers granted under PECA, the Pakistani government has provided little public information about its defensive cybersecurity capabilities against external threats. And while Pakistan's cabinet approved a National Cybersecurity Policy in 2021, the bill suffers from several critical drawbacks. Critics have argued that the policy has arrived far too late, in a landscape that is already marred by serious data breaches – such as those at the FBR and NADRA mentioned earlier in this study – due to institutional negligence and failure to act on audit warnings.[62] A key issue is the lack of seriousness within government departments, where basic cybersecurity practices are often ignored, and digital security spending is viewed as unnecessary. Despite acknowledging the need for capacity-building and behavioral change, the policy provides only vague timelines and offers no clear roadmap for overcoming bureaucratic resistance. Enforcement remains weak, with laws like PECA poorly implemented and grossly misused by agencies such as the FIA, which suffer from inefficiency, missing evidence, and lack of trained personnel.

Crucially, there is no functioning data protection law in Pakistan, leaving citizens vulnerable and deterring foreign investors. The policy's emphasis on data localisation also ignores the global nature of the internet and risks undermining encryption protocols essential for securing sensitive data. Furthermore, it lacks clear mechanisms for accountability and fails to ensure the inclusion of diverse stakeholders, raising doubts about its long-term effectiveness. While the National Cybersecurity Policy proposes ambitious reforms – from special cyber courts to cybersecurity education – its success will depend on deep structural reform, legal clarity, and sustained cross-sector collaboration.[63] This lack of transparency raises critical questions about whether adequate infrastructure exists to protect against sophisticated state-sponsored attacks and whether the extensive data collection under PECA actually enhances national security or merely creates larger databases vulnerable to external breaches.

The information vacuum itself demonstrates the broader problem of secrecy around cybersecurity policy in Pakistan. Without public accountability mechanisms, citizens cannot assess whether their privacy sacrifices under PECA have yielded meaningful security improvements or whether the government even possesses the technical capacity to protect the vast amounts of personal data it collects.

---

[62] Usama Khilji, 'Cybersecurity policy,' DAWN, 21 August 2021, https://www.dawn.com/news/1641754 (accessed on 1 September 2025)

[63] Ibid

As constitutional law expert Umer Gilani points out, "the more evident threats to data privacy don't emanate from this legislation. It is from the executive actions." He specifically references contracts that the PTA has signed for systems like "LIMS [or] Pegasus [or] Sandvine" and questions "whether these contracts are within the PTA's legislative framework or not." It is pertinent to note that LIMS enables authorities to conduct warrantless interception of citizens' communications data. The rolling out of LIMS highlights how surveillance capabilities often expand through executive decisions of "dubious constitutional legal validity" – passed through executive orders, rather than through transparent legislative processes.[64]

The vulnerability of Pakistani citizens' data extends beyond government surveillance to include significant data breaches. Gilani notes that "historically, the major breaches are from telecom data as a result of it, you can just go to SIMs databases online and other places and dig up anyone's phone number. And then, you know, you can get addresses, you can check whether they're a voter, an active taxpayer." There have been major data breaches in the past in Pakistan. Most notably, a major data breach in 2020 revealed that data of 115 million Pakistani mobile users was up for sale on the dark web with a price tag of $2.1 million.[65]

Pakistan's overall approach to cybersecurity and cyber intrusive technology prioritizes sovereignty and national security while selectively engaging with global cyber governance frameworks.[66] It has not acceded to multilateral treaties such as the Budapest Convention on Cybercrime – the only binding international instrument addressing cybercrime and electronic evidence – citing concerns over external jurisdiction and data sovereignty.[67] Conversely, Pakistan aligns with United Nations-led processes like the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE), which affirm the applicability of the UN Charter in cyberspace while preserving state autonomy.[68]

---

[64] Umer Ali & Ramsha Jahangir, 'Pakistan moves to install nationwide 'web monitoring system'' .Coda, 24 October 2019, https://www.codastory.com/authoritarian-tech/pakistan-nationwide-web-monitoring/ (accessed on 1 September 2025)
[65] Saima Shabbir, 'Pakistan investigates claims of mega mobile users data breach,' Arab News, 13 April 2020, https://www.arabnews.pk/node/1657621/pakistan (accessed on 1 September 2025)
[66] Gulraiz Iqbal, 'How Does International law Byte into Pakistan's Cyber Governance,' South Asian Voices, 24 June 2025, https://southasianvoices.org/geo-m-pk-r-cyber-governance-6-24-2025/ (accessed on 1 September 2025)
[67] Business Recorder, 'Pakistan not signed 'Budapest Convention' on cybercrime: LHC told,' Business Recorder, 1 February 2020, https://www.brecorder.com/news/567018 (accessed 1 September 2025)
[68] Gulraiz Iqbal, 'How Does International law Byte into Pakistan's Cyber Governance,' South Asian Voices, 24 June 2025, https://southasianvoices.org/geo-m-pk-r-cyber-governance-6-24-2025/ (accessed on 1 September 2025)

Recommendations

Redirecting Government Spending

Government funding should be strategically redirected away from offensive intrusive and mass surveillance capabilities - a trend that is all the more common nowadays given the substantial and staggering increase in technology that encourages citizens themselves to spy on their fellow citizens through invasive applications and peer tracking. Instead, the government should think about spending towards data protection legislation and building cybersecurity capabilities.

Multi-Stakeholder Collaboration

Digital rights experts in Pakistan emphasize the critical need for multi-stakeholder collaboration to effectively address cyber intrusive technology misuse. As Ramsha Jehangir noted, "more multi stakeholder collaboration... coming together, lawyers coming together, like more multi stakeholder collaboration, I think is powerful, because then you're basically helping each other understand the different gaps that you wouldn't otherwise working in silos." Rather than working in organizational silos, civil society organizations, journalists, lawyers, and affected communities must coordinate their efforts to leverage complementary expertise and create sustained pressure for reform. This collaborative approach has proven minimally effective in recent advocacy campaigns, particularly around PECA amendments, where unified opposition from diverse stakeholders generated unprecedented public attention and media coverage.

Experts recommend shifting focus from government-centric approaches toward citizen-centered advocacy that prioritizes the experiences of those most affected by surveillance technologies. Jehangir emphasizes "reframing the focus on citizens, but also other stakeholders are impacted. So journalists, activists, women like communities, who are on the receiving end of this." This includes journalists, activists, women, and marginalized communities who face disproportionate targeting through cyber intrusive tools. Given the limited success of traditional government engagement, which often devolves into tokenistic consultations, civil society should concentrate on building awareness and protective capacity among vulnerable populations while simultaneously documenting violations for future advocacy use.

Communication and Public Engagement Strategies

Shmyla Khan emphasizes the importance of being able to "demystify" actions that the government is taking, and communicate the impact of cyber-surveillance technologies in "everyday terms" rather than relying on legalistic language about privacy violations so that they resonate better with broader audiences. Advocates should focus on tangible impacts such as infrastructure disruption, economic consequences, and specific examples of government overreach. This approach proved successful during recent internet slowdowns in Pakistan, when widespread public frustration created unprecedented pressure for government accountability.

Experts also emphasize the importance of providing citizens with specific, actionable questions they can ask about surveillance programs, and providing specific cost estimates for surveillance systems to make issues tangible. Making technical issues accessible through clear explanations of how surveillance systems function and their implications for ordinary citizens can help build the informed public discourse necessary for sustained advocacy efforts.

Legal and Parliamentary Pathways

In the fast-paced technology industry, companies are constantly evolving their cyber-surveillance tools leaving important stakeholders in the lurch about how to deal with emerging, advancing threats in real time. To deal with the effects of cyber-surveillance efficiently, the government needs to strengthen its approach by following established frameworks like the NIST Cybersecurity Framework[1], which has become the gold standard for managing cyber risks through public-private collaboration.

Alongside such concrete frameworks in place, and despite significant limitations and intimidation tactics, experts recommend continuing strategic litigation and parliamentary engagement as important components of a comprehensive advocacy strategy. While immediate legal remedies may be limited, court cases serve crucial functions in creating public records, establishing precedents, and forcing government acknowledgment of surveillance practices. The audio leaks case in the Islamabad High Court, for instance, resulted in the first official acknowledgment of LIMS, even though the government subsequently issued notifications providing legal cover for these activities. As Jehangir notes, it's important to put "on record for advocacy purposes... [that] this was illegal or unconstitutional" even when immediate remedies aren't available.

Even when immediate policy changes are unlikely, creating documented records of government responses to parliamentary questions establishes important precedents for future advocacy efforts. However, digital rights expert Usama Khilji cautions that "the real question is, are political parties willing to fight that fight? And the answer is [often] no" due to their dependence on establishment approval.

International Collaboration and Pressure

Given domestic constraints on advocacy effectiveness, experts emphasize the crucial role of international collaboration and pressure mechanisms. This includes engaging with UN Human Rights Council special procedures, leveraging trade relationships such as GSP+ status requirements, and building solidarity with digital rights movements in other countries facing similar challenges. Jehangir highlights the importance of "getting more international allies to help support local advocacy" and notes that "international coverage or access... probably will have more impact" than purely domestic efforts. International media coverage and diplomatic pressure have proven effective in recent cases, particularly when combined with strong domestic advocacy.

Regional collaboration offers particular promise, as many South Asian countries face similar patterns of surveillance expansion and legal frameworks that prioritize state security over individual privacy. Jehangir recommends "finding cross collaboration and those common patterns" and notes that "a lot of places are going through the same thing" with regards to cyber intrusive technology deployment. Sharing advocacy strategies, legal precedents, and technical expertise across borders can strengthen domestic movements while building broader coalitions for digital rights protection. Cross-regional learning also helps identify common patterns in how surveillance technologies and supporting legal frameworks spread between countries, enabling more effective counter-strategies.

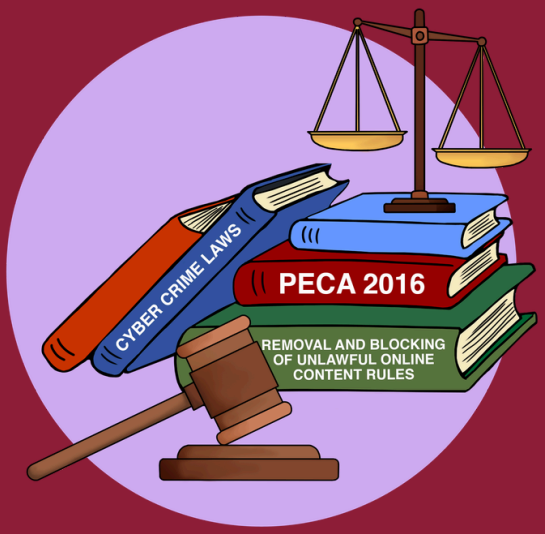
Sustained Advocacy

Experts stress that addressing cyber intrusive technology requires sustained, long-term advocacy rather than reactive responses to specific incidents. This includes systematic documentation of violations, building institutional memory within civil society organizations, and maintaining pressure even when immediate policy changes seem unlikely. The gradual expansion of surveillance capabilities and legal frameworks occurs over years or decades, requiring equally persistent advocacy efforts to counter these trends.

Documentation serves multiple purposes beyond immediate advocacy goals, including building evidence bases for future legal challenges, educating new generations of advocates, and creating historical records that can inform policy discussions when political opportunities emerge. Even when government responses are limited or hostile, maintaining consistent pressure through multiple channels creates cumulative effects that can contribute to longer-term change.

Conclusion - Towards a More Balanced Approach

Despite serious privacy implications, Pakistan has failed to implement comprehensive data protection legislation. Although the MoITT drafted the Personal Data Protection Bill in 2018 – which would have established data protection standards, created a dedicated authority, and defined individual rights – the bill remains tabled despite years of discussions.



This legislative gap creates significant vulnerabilities for Pakistani citizens, whose personal data may be collected, processed, shared, or exposed without adequate legal protections or remedies, a particularly troubling situation given Pakistan's rapid digitization and increasing instances of data breaches and cyber intrusions.

In the name of national security, PECA has created a powerful surveillance state with minimal privacy protections or oversight mechanisms, demonstrating how emergency legislation enacted during times of crisis often prioritizes state power at the expense of fundamental rights. Today, Pakistani citizens remain uniquely vulnerable to both government-sanctioned cyber intrusion and malicious data breaches from external actors. The combination of extensive data collection under PECA, minimal restrictions on how that data can be used or shared, and the absence of comprehensive data protection legislation has created a perfect storm where personal data exists in a state of permanent jeopardy.

Without meaningful reforms that balance legitimate security concerns with robust privacy protections, Pakistan risks normalizing a surveillance culture where neither citizens' data nor their fundamental rights receive the protection they deserve under international human rights frameworks and the state’s own constitution.

This scoping study reveals significant gaps in our understanding of Pakistan's cyber intrusive technology deployment landscape, particularly regarding defensive capabilities, international cooperation, and policy implementation. Future research should focus on filling these knowledge gaps while continuing to monitor the impact of existing surveillance laws on civil liberties and democratic governance. Only through such comprehensive analysis can Pakistan develop policies that genuinely protect both national security and citizens' fundamental rights.

Works Cited

“Pakistan passes controversial cyber-crime law.” Reuters, August 12, 2016, https://www.reuters.com/article/us-pakistan-internet-idUSKCN10N0ST/

“Prevention of Electronic Crimes Act, 2016” National Assembly of Pakistan, https://www.na.gov.pk/uploads/documents/1470910659_707.pdf

Abbas, Zaki. “The surveillance system keeping tabs on millions.” DAWN. July 2, 2024, https://www.dawn.com/news/1843299

Abdullah, Hasan. “Fishing in troubled waters.” DAWN, April 26, 2015, https://www.dawn.com/news/1177605/fishing-in-troubled-waters

Ali, Umer, and Jehangir, Ramsha. “Pakistan moves to install nationwide “web monitoring system.”” .Coda, October 14, 2019, https://www.codastory.com/authoritarian-tech/pakistan-nationwide-web-monitoring/

Amin, Tahir. “AIC raises questions about ‘Pakistan Draft Data Protection Bill 2023.” Business Recorder, July 24, 2023, https://www.brecorder.com/news/40254218/aic-raises-questions-about-pakistan-draft-data-protection-bill-2023

Amnesty International Security Lab. “To Catch a Predator: Leak exposes the internal operations of Intellexa’s mercenary software.” Amnesty International, December 1, 2025. https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed/

Amnesty International. “Pakistan: Campaign of hacking, spyware and surveillance targets human rights defenders.” Amnesty International, May 23, 2018, https://www.amnesty.org/en/latest/news/2018/05/pakistan-campaign-of-hacking-spyware-and-surveillance-targets-human-rights-defenders/

Amnesty International. “Shadows of Control: Censorship and mass surveillance in Pakistan.” Amnesty International, September 9, 2025, https://www.amnesty.org/en/documents/asa33/0206/2025/en/

Aziz, Farieha. “Pakistan’s cybercrime law: boon or bane?” Heinrich Böll Stiftung, May 7, 2025, https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

Baig, Asad. “2900% increase in Pakistan government’s requests for Facebook ‘user data’ in last 5 years.” Digital Rights Monitor, December 21, 2017, https://digitalrightsmonitor.pk/2900-increase-in-pakistan-governments-requests-for-facebook-user-data-in-last-5-years

Bakhtiar, Idrees, and Abbas, Zaffar. “The mysterious case of Operation Midnight Jackal.” Herald Magazine. November 19, 2018, https://herald.dawn.com/news/1398719

BlackBerry. “Global threat intelligence report: August 2023.” Blackberry, August 2023, https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/bbcomv4/blackberry-com/en/solutions/threat-intelligence/2023/threat-intelligence-report-august/Blackberry-Global-Threat-Intelligence-Report-August-2023.pdf

BlackBerry. “SideWinder uses server-side polymorphism to target Pakistan.” Blackberry, May 8, 2023, https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan

Business Recorder. “Digitalisation: World Bank VP briefed on FBR’s initiatives.” Business Recorder, May 9, 2024, https://www.brecorder.com/news/40302562/digitalisation-world-bank-vp-briefed-on-fbrs-initiatives

Business Recorder. “Pakistan not signed ‘Budapest Convention’ on cybercrime: LHC told.” Business Recorder, January 31, 2020, https://www.brecorder.com/news/567018

Chaudhri, Adnan. “Spectrum Eyes: The NSA & Pakistani Metadata.” Digital Rights Foundation, May 14, 2015. https://digitalrightsfoundation.pk/spectrum-eyes-the-nsa-pakistani-metadata/

Chaudhry, Noor Ejaz. “Big Brother: Mapping State Surveillance of Citizens Online and Offline.” Digital Rights Monitor. February 8, 2021. https://digitalrightsmonitor.pk/pakistan-as-big-brother-mapping-state-surveillance-of-citizens-online-and-offline/

Cloudflare, “What is data localization?” Cloudflare, https://www.cloudflare.com/en-gb/learning/privacy/what-is-data-localization/

Committee to Protect Journalists. “Pakistan court remands journalist Asad Ali Toor in cybercrime case.” Committee to Protect Journalists, March 15, 2024, https://cpj.org/2024/03/pakistan-court-remands-journalist-asad-ali-toor-in-cybercrime-case/

Craig, Tim, and Hussain, Shaiq. “Pakistan’s mobile phone owners told: be fingerprinted or lose your sim cards.” The Guardian, March 3, 2015, https://www.theguardian.com/world/2015/mar/03/pakistan-fingerprint-mobile-phone-users

DAWN “Surveillance in Pakistan exceeds legal capacity: report.” DAWN, July 22, 2015 https://www.dawn.com/news/1195668

Dawn. “PTA says it does not conduct surveillance.” DAWN, May 7, 2014, https://www.dawn.com/news/1104784

Dedola, Giampaolo, and Bernikov, Vasily. “SideWinder targets the maritime and nuclear sectors with an updated toolset.” Securelist, March 10, 2025, https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/

Dedola, Giampaolo, and Bernikov, Vasily. “SideWinder targets the maritime and nuclear sectors with an updated toolset.” Securelist, March 10, 2025, https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/

Digital Rights Foundation. “Voter data privacy in Pakistan: Privacy risks, data protection, and legislative shortcomings during data-driven elections.” Digital Rights Foundation. January 2025, https://digitalrightsfoundation.pk/wp-content/uploads/2025/01/Voter-Data-Privacy-in-Pakistan.pdf

Fazal, Maham. “General Zia-Ul-Haq’s Dark Legacy: How One Man Rewired The Soul of Pakistan.” The Friday Times, July 5, 2025, https://www.thefridaytimes.com/05-Jul-2025/general-zia-ul-haq-s-dark-legacy-how-one-man-rewired-the-soul-of-pakistan

Google Transparency Report. “Government requests to remove content removal requests – Pakistan.” Google, https://transparencyreport.google.com/government-removals/government-requests/PK

Gul, Ayaz. “Mystery Around Audio Leaks from Pakistan PM’s Office Deepens.” Voice of America, October 10, 2022, https://www.voanews.com/a/mystery-around-audio-leaks-from-pakistan-pm-s-office-deepens-/6783855.html

Guramani, Nadir. “NA informed Web Monitoring System deployed to block applications, websites not in agreement with law.” DAWN, August 30, 2024. https://www.dawn.com/news/1855782

Haque, Jahanzaib. “Customer 32 — who used FinFisher to spy in Pakistan?” DAWN, August 24, 2014, https://www.dawn.com/news/1127405

Human Rights Library. “Cairo Declaration on Human Rights in Islam,” University of Minnesota, http://hrlibrary.umn.edu/instree/cairodeclaration.html

Husain, Irfan. “Rush to judgement.” DAWN. February 10, 2001. https://www.dawn.com/news/1072392

Hussain, Abid. “Pakistan tests secret China-like ‘firewall’ to tighten online surveillance.” Al Jazeera, November 26, 2024, https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance

Hussain, Abid. “Why is Pakistan investigating several audio leaks from PM office?” Al Jazeera, September 29, 2022, https://www.aljazeera.com/news/2022/9/29/why-is-pakistan-investigating-several-audio-leaks-from-pm-office

Hussain, Javed. “Nadra’s biometric data has been compromised, FIA official tells NA body.” DAWN, November 25, 2021, https://www.dawn.com/news/1660199

Integrated Research, “Deep Packet Inspection (DPI): How it works and why it’s important.” Integrated Research, https://www.ir.com/guides/deep-packet-inspection

International Federation of Journalists. “Pakistani government monitoring journalists’ social media activity.” International Federation of Journalists, April 1, 2019, https://www.ifj.org/media-centre/news/detail/article/pakistani-government-monitoring-journalists-social-media-activity

Iqbal, Gulraiz. “How Does International Law Byte into Pakistan’s Cyber Governance?” South Asian Voices, June 24, 2025, https://southasianvoices.org/geo-m-pk-r-cyber-governance-6-24-2025/

Iqbal, Sahar. “Legal landscape for privacy and surveillance in Pakistan.” International Bar Association, June 20, 2023, https://www.ibanet.org/legal-landscape-for-privacy-surveillance-in-Pakistan

Iqbal, Sahar. “The right to be forgotten in Pakistan.” International Bar Association, August 22, 2023, https://www.ibanet.org/the-right-to-be-forgotten-in-Pakistan

Khan, Eesha Arshad. “The prevention of electronic crimes act 2016: An analysis.” SAHSOL LUMS, https://sahsol.lums.edu.pk/node/12862

Khan, Naimat. “Pakistan government monitoring journalists' social media activity.” Arab News, April 8, 2025, https://www.arabnews.com/node/2596269/pakistan

Khan, Sher Ali. “The state bytes back: Internet surveillance in Pakistan.” Herald Magazine, May 23, 2017, https://herald.dawn.com/news/1153312#top

Khilji, Usama. “Cybersecurity policy.” DAWN, August 21, 2021, https://www.dawn.com/news/1641754

Khilji, Usama. “Silencing Pakistan.” DAWN, July 28, 2023, https://www.dawn.com/news/1767243

Kumar, Abhishek. “Revisiting the Nuclear Nexus between Pakistan, China, and North Korea.” Institute for Security and Development Policy, January 5, 2003. https://www.isdp.eu/revisiting-the-nuclear-nexus-between-pakistan-china-and-north-korea/

Library of Congress. “Pakistan: National Assembly Passes New Cybercrime Law.” Library of Congress, September 21, 2016, https://www.loc.gov/item/global-legal-monitor/2016-09-21/pakistan-national-assembly-passes-new-cybercrime-law/

Marquis-Boire, Morgan, Marczak, Bill, Guarnieri, Claudio, and Scott-Railton, John. “For Their Eyes Only: The Commercialization of Digital Spying.” Citizen Lab, May 1, 2013, https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

Mehtab, Umer. “Audio leaks case: IHC dismisses IB’s petition to withdraw plea seeking Justice Sattar’s recusal.” DAWN, May 3, 2024, https://www.dawn.com/news/1831190

Mehtab, Umer. “IHC says those involved in and aiding surveillance of citizens are “liable for offences.”” DAWN, May 30, 2024, https://www.dawn.com/news/1836404

Momand, Abdullah. “SC suspends IHC order in audio leaks case, bars court from further proceedings.” DAWN, August 19, 2024, https://www.dawn.com/news/1853303

Mukerjee, Dilip. “Zia’s Military Legacy.” The Round Table: The Commonwealth Journal of International Affairs and Policy Studies, 310, no. 78 (1989): 179-191. https://doi.org/10.1080/00358538908453924

NACTA. “Investigation for Fair Trial Act, 2013.” National Counter Terrorism Authority, https://nacta.gov.pk/wp-content/uploads/2017/09/INVESTIGATION-FOR-FAIR-TRIAL-ACT.2013.pdf

NEWS DESK. (2020, August 14). Major cyber attack by Indian intelligence identifiedISPR. The Express Tribune. https://tribune.com.pk/story/2259193/major-cyber-attack-by-indian-intelligence-identified-ispr

NIST, “Cybersecurity Framework,” https://www.nist.gov/cyberframework

Office of United Nations High Commissioner for Human Rights. “Convention on the Rights of the Child.” United Nations. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

Office of United Nations High Commissioner for Human Rights. “International Covenant on Civil and Political Rights.” United Nations. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Pakistan Telecommunications Authority, “Pakistan Telecommunication (Re-Organization) Act, 1996.” PTA, https://www.pta.gov.pk/assets/media/pta_act_consolidated_footnotes_11012022.pdf

Privacy International. “Pakistan: Intelligence agency sought to tap all communications traffic, documents reveal.” Privacy International. July 21, 2015. https://privacyinternational.org/blog/1364/pakistan-intelligence-agency-sought-tap-all-communications-traffic-documents-reveal

Privacy International. “Pirvacy International raises concerns regarding Pakistan’s Personal Data Protection Bill.” Privacy International, August 8, 2023. https://privacyinternational.org/news-analysis/5090/privacy-international-raises-concerns-regarding-pakistans-personal-data

Privacy International. “Punjab government's Safe Cities Project: Safer city or over-policing?” Privacy International, March 20, 2018, https://privacyinternational.org/news-analysis/2228/punjab-governments-safe-cities-project-safer-city-or-over-policing

Privacy International. “Timeline: SIM card registration laws in Pakistan.” Privacy International, October 17, 2019, https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws

Privacy International. “Timeline: SIM card registration laws in Pakistan.” Privacy International, October 17, 2019, https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws

Privacy law library. (n.d.). Retrieved 7 May 2025, from https://privacylibrary.ccgnlud.org/case/mohtarma-benazir-bhutto-and-ors-vs-president-of-pakistan-and-or

Privacy law library. (n.d.). Retrieved 7 May 2025, from https://privacylibrary.ccgnlud.org/case/mohtarma-benazir-bhutto-and-ors-vs-president-of-pakistan-and-or

Rana, Shahbaz. “Neglect caused FBR cyber attack.” The Express Tribune, August 22, 2021, https://tribune.com.pk/story/2316604/neglect-caused-fbr-cyber-attack

Rashid, Sohail. “SC hears Benazir Bhutto’s 1997 phone tapping review plea against President Leghari.” Samaa TV, December 11, 2024, https://www.samaa.tv/index.php/2087325410-sc-hears-benazir-bhutto-s-1997-phone-tapping-review-plea-against-president-leghari

Sangfor Technologies. “Suspected SideWinder APT attack on the Pakistan government.” Sangfor Technologies, June 12, 2023, https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/suspected-sidewinder-apt-attack-on-pakistan-government

Scahill, Jeremy, and Begley, Josh. “How Spies Stole the Keys to the Encryption Castle.” The Intercept. February 19, 2015, https://theintercept.com/2015/02/19/great-sim-heist/

Shabbir, Saima. “Pakistan investigates claims of mega mobile users data breach.” Arab News, April 12, 2020, https://www.arabnews.pk/node/1657621/pakistan

Shabbir, Saima. “Rights activists raise privacy concerns after Pakistan authorizes top spy agency to tap calls, messages.” Arab News, July 9, 2024, https://arab.news/c9732

Shehzad, Rizwan. “Govt defends legal cover for surveillance.” The Express Tribune, July 10, 2024, https://tribune.com.pk/story/2478373/govt-defends-legal-cover-for-surveillance

Shehzad, Rizwan. “High powered panel to probe audio leaks.” The Express Tribune. October 10, 2022, https://tribune.com.pk/story/2380194/high-powered-panel-to-probe-audio-leaks

Siddiqui, Tahir. “Real-time surveillance begins under Karachi Safe City project, CM told.” DAWN, November 20, 2024, https://www.dawn.com/news/1873508

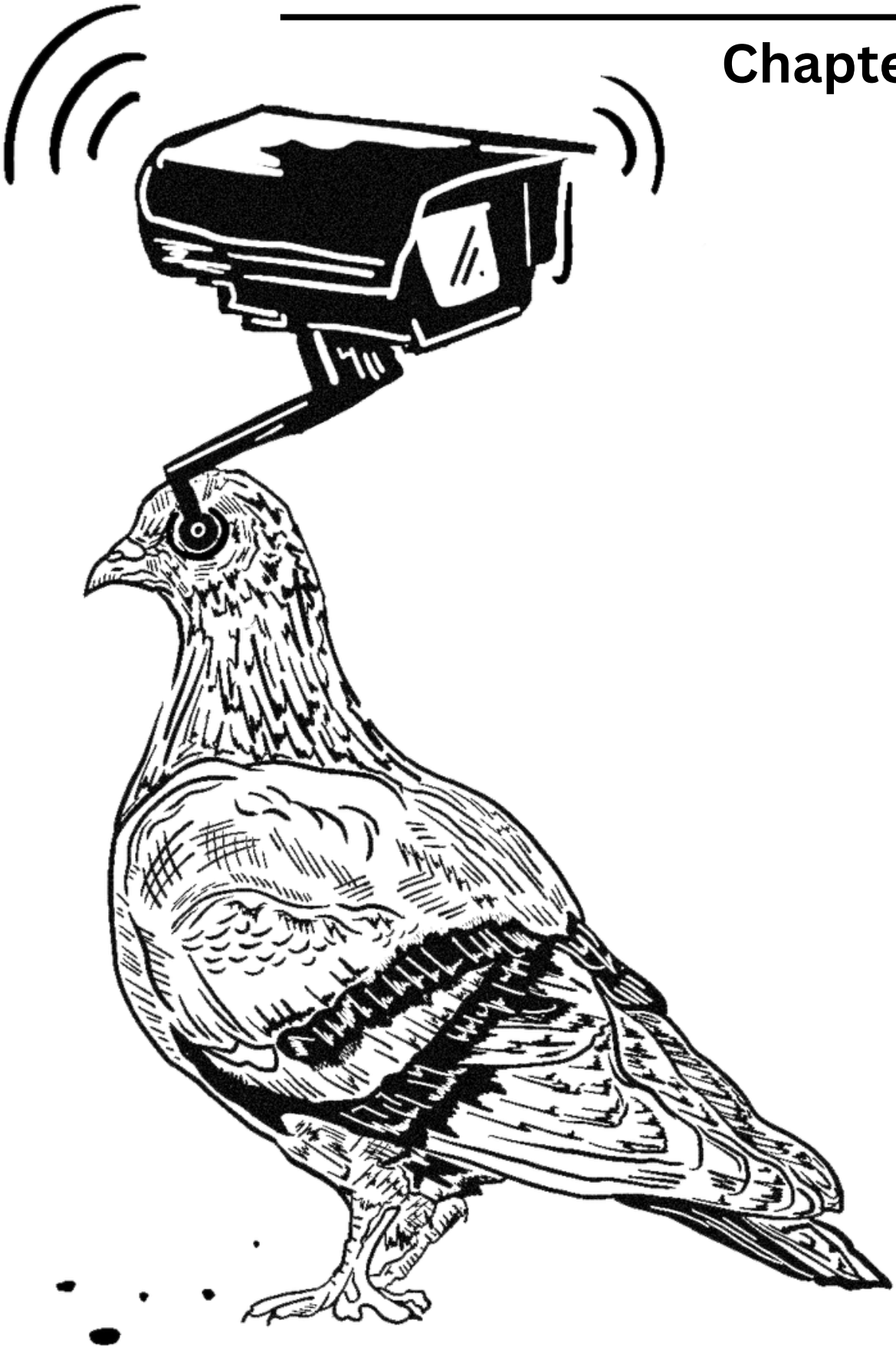
Team, B. R. a. I. (2023, May 8). SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is Now Targeting Turkey. Blackberry Blogs. https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan

United Nations “Universal Declaration of Human Rights” United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

VOA Urdu. “Pakistan hearings on surveillance, TikTok worry digital rights advocates.” Voice of America, July 8, 2024, https://www.voanews.com/a/pakistan-hearings-on-surveillance-tiktok-worry-digital-rights-advocates-/7689948.html

BANGLADESH

Chapter 2



DRF USA

Abbreviations

AL	Awami League
BDT	Bangladeshi Taka
BNP	Bangladesh Nationalist Party
BTRC	Bangladesh Telecommunication Regulatory Commission
CSA	Cyber Security Act
DGFI	Directorate General of Forces Intelligence
DoT	Department of Telecommunication
DPI	Deep Packet Inspection
DSA	Digital Services Act
ICT Act	Information and Communication Technology Act (2006)
ILIS	Integrated Lawful Interception System
ISP	Internet Service Provider

NSI	National Security Intelligence
NTMC	National Telecommunication Monitoring Centre
RAB	Rapid Action Battalion
RAW	Research and Analysis Wing
UFED	Universal Forensic Extraction Devices

Introduction

In the contemporary digital era, states—particularly in the Global South—have increasingly conflated national security imperatives with political consolidation through advanced surveillance technologies. Bangladesh exemplifies this dynamic: while successive governments have justified the gradual construction of a cyber intrusion apparatus by citing terrorism and public-order concerns, in practice, these tools have facilitated deeper political control and infringed on citizens' right to privacy and freedom of expression.

The roots of modern surveillance in Bangladesh trace back to post-independence authoritarianism, when intelligence activities relied on human informants, analog wiretapping, and colonial-era statutes such as the Telegraph Act of 1885 and the Official Secrets Act of 1923 .[1] The institutional expansion of agencies like the Directorate General of Forces Intelligence (DGFI) and National Security Intelligence (NSI) followed critical security crises, most notably the assassinations of presidents, Sheikh Mujibur Rahman (1975) and Ziaur Rahman (1981).

[1] Zakir Hossain, 'INTELLIGENCE AND NATIONAL SECURITY: BANGLADESH PERSPECTIVE,' The Indian Journal of Political Science, Volume 78, No. 3, September 2017 https://www.jstor.org/stable/26535023 (accessed on 1 September 2025)

With the restoration of parliamentary democracy in 1991, surveillance gained formal legitimacy but became increasingly politicized amid an intense rivalry between the Bangladesh Nationalist Party (BNP) and the Awami League (AL).[2] After the September 11 attacks in the United States, counterterrorism imperatives prompted creation of elite units such as the Rapid Action Battalion (RAB) in Bangladesh, endowed with expansive interception and enforcement powers. Since 2009, the AL government has overseen the rapid digitization of surveillance infrastructure—through bodies including the National Telecommunication Monitoring Centre (NTMC) and the Counter Terrorism and Transnational Crime unit—often deploying foreign-supplied technologies.[3]

Although counterterrorism and national security remains the stated rationale behind state surveillance and interception even today, mounting evidence demonstrates that these capabilities have been repurposed to monitor opposition figures, journalists, and activists—particularly during the disputed 2014 and 2018 elections.[4] The July–August 2024 uprisings further revealed the regime's readiness to employ digital surveillance alongside internet blackouts and warrantless device seizures.

[2] Ali Riaz, 'Bangladesh: A Political History since Independence,' Bloomsbury Publishing, 2016

[3] Mubashar Hasan, 'Democracy and Political Islam in Bangladesh,' South Asia Research, Volume 31, No. 2, https://doi.org/10.1177/026272801103100201 (accessed on 1 September 2025)

[4] 'BTRC blocks Skype,' The Daily Star, 19 November 2018, https://www.thedailystar.net/js-polls-2018/btrc-blocks-skype-1662676 (accessed on 1 September 2025)

This scoping study thus seeks to unpack central questions around what cyber surveillance tools and technologies have been deployed by the Bangladeshi government, how they were acquired, and to what extent do existing legal and institutional frameworks regulate—or fail to regulate—the use of these surveillance capabilities.

Historical Context

Bangladesh's surveillance system, rooted in colonial-era policing traditions, has evolved from rudimentary, human-led intelligence gathering into a sophisticated cyber infrastructure shaped by authoritarian politics, internal security failures, military intelligence priorities, and global counterterrorism agendas. This evolution spans institutions, laws, and technological capabilities, reflecting a persistent pattern of state control often at the expense of fundamental rights and freedoms. Over the last two decades, successive governments have expanded surveillance powers under the guise of national security and public order, disproportionately targeting dissenters, activists, journalists, and opposition parties, with the July-August 2024 mass uprising highlighting both the extensive reach of the surveillance apparatus and its misuse in suppressing dissent. As Bangladesh undergoes democratic transition, it remains a challenge for the interim government to ensure structural reforms that balance security imperatives with the protection of individual rights, such as the right to privacy and dignity, and democratic principles. The challenge is compounded by the absence of a deeper historical and ideological context to anchor these reforms.

After gaining independence in 1971, Bangladesh saw successive autocratic and semi-autocratic governments, with regimes throughout the mid- and late-twentieth century primarily relying on human intelligence and wiretapping for state surveillance, sanctioned by colonial-era or -inspired statutes (for instance, inter alia, the Code of Criminal Procedure, 1898, the Special Powers Act, 1974, the Telegraph Act, 1885, and the Wireless Telegraphy Act, 1933). During this period, key intelligence agencies, such as DGFI, NSI, and the various intelligence wings of Bangladesh Police, were either established or expanded, particularly in response to significant intelligence failures, including two presidential assassinations.[5] Until the early 1990s, the security apparatus predominantly targeted civil society activists, leftist groups, labor and trade unions, intellectuals, student organizations, political opponents and opposition parties, and other groups perceived as disloyal to the regime.[6] As Bangladesh transitioned to parliamentary democracy in 1991, surveillance was increasingly institutionalized through legislative and executive measures, amid escalating political tension between the Bangladesh Nationalist Party (BNP) and the Bangladesh Awami League (AL).[7]

---

[5] Zakir Hossain, 'INTELLIGENCE AND NATIONAL SECURITY: BANGLADESH PERSPECTIVE,' The Indian Journal of Political Science, Volume 78, No. 3, September 2017 https://www.jstor.org/stable/26535023 (accessed on 1 September 2025)

[6] Sumit Ganguly, 'The Rise of Islamist Militancy in Bangladesh,' United States Institute of Peace, August 2006, https://www.files.ethz.ch/isn/39241/2006_august_sr171.pdf (accessed on 1 September 2025)

[7] Zakir Hossain, 'INTELLIGENCE AND NATIONAL SECURITY: BANGLADESH PERSPECTIVE,' The Indian Journal of Political Science, Volume 78, No. 3, September 2017 https://www.jstor.org/stable/26535023 (accessed on 1 September 2025)

Since then, the primary catalyst for expanding surveillance capabilities in Bangladesh was the rise of militancy.[8] Following the events of September 11, 2001, prevailing narratives at the time from across the globe found Bangladesh in the spotlight as one of the potential hotspots for terrorist sleeper cells and extremist recruitment, with groups such as Harakat ul-Jihadi-Islami, Jamaatul Mujahedin, and Hizb ut-Tahrir drawing particular attention.[9] Notably, BNP's second term coincided with the attacks on September 11, which established counterterrorism as a dominant paradigm in international relations worldwide. Against this backdrop, several high-profile terror incidents within Bangladesh intensified international pressure on the BNP-led government, resulting in the proscription of terrorist organizations and the prosecution of their leaders. These included the attempted assassination of the British High Commissioner and the 2004 grenade attack targeting former Prime Minister Sheikh Hasina, as well as the 2005 coordinated bombings across 300 locations in 63 out of the 64 districts, each carried out by or linked to Harakat ul-Jihadi-Islami and Jamaatul Mujahedin.[10] Additionally, it was also alleged that the United Liberation Front of Assam and other anti-India insurgency groups operated from Bangladesh.[11] In these contexts, the BNP-led government expanded state surveillance and security powers through legislative reforms that institutionalized broad surveillance mandates and granted RAB extensive authority to conduct intelligence operations.[12]

---

[8] Sumit Ganguly, 'The Rise of Islamist Militancy in Bangladesh,' The Center for Conflict Analysis and Prevention of the United States Institute of Peace, August 2006, https://www.files.ethz.ch/isn/39241/2006_august_sr171.pdf (accessed on 1 September 2025)

[9] United States Department of State, 'Country Reports on Terrorism 2007,' United States Department of State, April 2008, https://2009-2017.state.gov/documents/organization/105904.pdf (accessed on 1 September 2025)

[10] Sumit Ganguly, 'The Rise of Islamist Militancy in Bangladesh,' The Center for Conflict Analysis and Prevention of the United States Institute of Peace, August 2006, https://www.files.ethz.ch/isn/39241/2006_august_sr171.pdf (accessed on 1 September 2025)

Crisis Group, 'Political Conflict, Extremism and Criminal Justice in Bangladesh,' Crisis Group, April 2016, https://crisisgroup.org/sites/default/files/277-political-conflict-extremism-and-criminal-justice-in-bangladesh.pdf (accessed on 1 September 2025)

Ryan Clarke & Shafqat Munir 'Avoiding Suicide Terrorism in Bangladesh,' Combating Terrorism Center at West Point, May 2009, https://ctc.westpoint.edu/avoiding-suicide-terrorism-in-bangladesh/ (accessed on 1 September 2025)

[11] United States Department of State, 'Country Reports on Terrorism 2007,' United States Department of State, April 2008, https://2009-2017.state.gov/documents/organization/105904.pdf (accessed on 1 September 2025)

[12] Fred Abrahams, 'Judge, Jury and Death: Torture and Extrajudicial Killings by Bangladesh's Elite Secuirty Forces,' Human Rights Watch, 6 June 2006, https://www.hrw.org/reports/2006/bangladesh1206/bangladesh1206.htm (accessed on 1 September 2025)

From 2009 onwards, the AL government, over four consecutive terms, acquired sophisticated surveillance technologies and trained enforcement agencies in their use.[13] India's foreign intelligence agency, the Research and Analysis Wing (RAW)—although active in Bangladesh since the country's independence—reportedly strengthened its alliance with the domestic intelligence community in Bangladesh under the AL-led government.[14] This infrastructure of digital surveillance, interception, and online monitoring expanded significantly during these successive regimes through a series of legal and institutional measures designed to consolidate state control over information flow, curtail dissent, and preempt political opposition.

While the surveillance infrastructure was originally aimed at countering national security threats from both domestic and foreign organized militancy (such as Ansar al-Islam, Islamic State, Harakat ul-Jihadi-Islami, and Hizb ut-Tahrir), it was deployed and expanded over the years to help consolidate AL's political power and suppress dissent. An investigation by Tech Global Institute conducted in 2025 found that, ahead of the national elections in 2018 and 2024, government spending on advanced surveillance and spyware rose over a 12-18-month period, with the largest single-year expenditure recorded in 2022 at nearly USD 88.3 million.[15] Before the 2018 election, most spending focused on geolocation trackers and related software. By 2023, the emphasis had shifted to spyware capable of remote eavesdropping, full device access, and data extraction.

---

[13] David Jackman, 'Dominating Dhaka,' Effective States and Inclusive Development Working Paper No. 127, November 2019, https://www.effective-states.org/wp-content/uploads/working_papers/final-pdfs/esid_wp_127_jackman.pdf (accessed on 1 September 2025)
C R Abrar, 'Machinations of a fearsome state,' The Daily Star, 1 January 2018, https://www.thedailystar.net/supplements/unpacking-2017/machinations-fearsome-state-1513066 (accessed on 1 September 2025)

[14] Sumit Ganguly, 'The Rise of Islamist Militancy in Bangladesh,' The Center for Conflict Analysis and Prevention of the United States Institute of Peace, August 2006, https://www.files.ethz.ch/isn/39241/2006_august_sr171.pdf (accessed on 1 September 2025)

[15] Tech Global Institute, 'The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh,' Tech Global Institute, August 2025, https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf (accessed on 1 September 2025)

This allegedly enabled the party to secure three consecutive election victories in 2014, 2018, and 2023—each marred by credible allegations of rigging. In particular, AL's political rivals, including BNP, were reportedly subject to extensive digital surveillance along with arbitrary arrests, enforced disappearances and extrajudicial killings.[16] These included location and movement tracking, phone tapping and call interception, and social media monitoring. These measures were also accompanied by other online curbs. For instance, ahead of the 2018 national elections, the government enforced a localized internet shutdown and blocked Skype to prevent opposition leaders from interviewing potential nominees.[17] Similarly, in 2022, mobile network services were deliberately degraded in areas hosting opposition rallies.[18] Amid this situation, the opposition had to withdraw from the electoral race on at least two occasions, once in 2014 and again exactly 10 years later in 2024.[19] Moreover, since its enactment, the Digital Security Act, 2018, has been used to justify arbitrary arrests and detentions of journalists, activists, students, and opposition figures.

[16] David Bergman, 'No Place for Criticism: Bangladesh Crackdown on Social Media Commentary,' Human Rights Watch, 9 May 2018, https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary (accessed on 1 September 2025)
OHCHR, 'Fact Finding Report: Human Rights Violations and Abuses related to the Protests of July and August 2024 in Bangladesh,' United Nations High Commissioner for Human Rights, 12 February 2025, https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf (accessed on 1 September 2025)

[17] 'BTRC blocks Skype,' The Daily Star, 19 November 2018, https://www.thedailystar.net/js-polls-2018/btrc-blocks-skype-1662676 (accessed on 1 September 2025)

[18] 'Mobile service disrupted as BNP rallies at Golapbagh,' The Financial Express, 10 December 2022, https://thefinancialexpress.com.bd/national/mobile-service-disrupted-as-bnp-rallies-at-golapbagh-1670654249 (accessed on 1 September 2025)

[19] Crisis Group Report, 'Beyond the Election: Overcoming Bangladesh's Political Deadlock,' Crisis Group, 4 January 2024, https://www.crisisgroup.org/asia/south-asia/bangladesh/336-beyond-election-overcoming-bangladeshs-political-deadlock (accessed on 1 September 2025)

During its consecutive reigns, the AL government not only deployed cyber-intrusive technologies—it significantly upgraded the state's surveillance capabilities. In 2018, the cabinet approved a multimillion-dollar deal to "strengthen tapping of phone and surveillance of social media" through procurement of systems from Ezy Infotech Pte Ltd, Spider Digital Innovation FZE, and Speedpial Trading LLC.[20] Around the same time, then State Minister for Information Tarana Halim and then Telecommunication Minister Mostafa Jabbar announced the formation of a social media monitoring unit to detect content that "threatens communal harmony, disturbs state security, or embarrasses the state" and reportedly allocated $11 million.[21] Similarly, in 2019, the NTMC reportedly also implemented a "Content Blocking and Filtering System."[22] In 2023, then Home Minister Asaduzzaman Khan acknowledged the existence of more sophisticated social media surveillance tools in the agency's inventory.[23] This increased investment in social media monitoring and content filtration systems in 2018-19 came in the backdrop of the nationwide road safety protests and the quota reform movement, as well as the national elections, when social media served as the main platform of mobilization that lay beyond the government's immediate control.

[20] 'Social media to come under telecom monitoring surveillance,' New Age, 13 June 2018, https://www.newagebd.net/article/43598/social-media-to-come-telecom-monitoring-surveillance (accessed on 1 September 2025)

[21] David Bergman, 'No Place for Criticism: Bangladesh Crackdown on Social Media Commentary,' Human Rights Watch, 9 May 2018, https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary (accessed on 1 September 2025)

Faisal Mahmud, 'Bangladesh ramps up efforts to monitor social media after months of student-led agitations,' Scroll, 21 August 2018, https://scroll.in/article/891011/bangladesh-ramps-up-efforts-to-monitor-social-media-after-months-of-student-led-agitations (accessed on 1 September 2025)

[22] 'NTMC will soon be able to block anti-govt propaganda,' The Daily Star, 21 February 2019, https://www.thedailystar.net/city/online-anti-govt-propaganda-in-bangladesh-ntmc-filter-1704910 (accessed on 1 September 2025)

[23] 'ARTICLE 19 condemns surveillance through controversial technology,' Dhaka Tribune, 17 January 2023, https://www.dhakatribune.com/bangladesh/302955/article-19-condemns-surveillance-throug (accessed on 1 September 2025)

Additionally, our findings show that the government invested close to USD 15 million in geolocation and device tracking by 2018, alongside USD 20-25 million in networking hardware and interception capabilities by 2019. These allocations rose substantially in the following years, with expanded spending across multiple categories. The surge culminated in the largest single-year expenditure on surveillance and spyware in 2022, totaling nearly USD 88.3 million.[24]

During the Monsoon Revolution in 2024, the AL government appears to have continued to rely on these capabilities to quell the mass uprising. According to a fact-finding report by the Office of the United Nations High Commissioner for Human Rights, the intelligence agencies "shared intelligence, including information obtained through surveillance in violation of the right to privacy, to enable the campaign of mass arbitrary arrest."[25] Specifically, the NTMC was found to have provided "surveillance and intelligence, including by monitoring people's personal communications and supporting arrest and other police operations." As this report is being written, the AL-led government has collapsed under the pressure of the Monsoon Revolution, and an interim government has been set up, whose first order of business in office has commenced a series of reform processes. In August 2025, the interim government announced the formation of a committee to investigate the expenditure on and the sources of surveillance equipment.[26] As this report is being written, there have been no updates and while it is unclear how this will play out in the coming months, current developments and past experiences do not inspire confidence in the new government, as even under the interim government, authorities have initiated procurement of a large-area signal scanner and a portable network surveillance kit, along with overseas training for government officials and the RAB on a mobile cell-interception system.[27]

---

[24] Tech Global Institute, 'The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh,' Tech Global Institute, August 2025, https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf (accessed on 1 September 2025)

[25] OHCHR, 'Fact Finding Report: Human Rights Violations and Abuses related to the Protests of July and August 2024 in Bangladesh,' United Nations High Commissioner for Human Rights, 12 February 2025, https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf (accessed on 1 September 2025)

[26] 'Govt to probe purchase of spy equipment during Hasina govt,' New Age, 14 August 2025, https://www.newagebd.net/post/country/273010/govt-to-probe-purchase-of-spy-equipment-during-hasina-govt (accessed on 1 September 2025)

[27] Tech Global Institute, 'The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh,' Tech Global Institute, August 2025, https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf (accessed on 1 September 2025)

Findings

Victims of Surveillance

In the most high-profile and internationally covered case, lawyer and activist Mir Ahmad bin Quasem was abducted in 2016 and put under arrest for over 8 years for speaking out against the then-government, along with multiple others who raised their voice in criticising the Bangladeshi state and its policies[28] - setting a dangerous precedent for the employment of surveillance technologies in the country. Almost 9 years later, human rights violations as an attempt to quash dissent in the country have been an ongoing predicament, creating a timeline that can specifically be tied to government spending patterns and legislation alike. A dangerous mix of readily available cyber arsenal in Bangladesh and controversial legislation, have given the government sweeping powers to track and record groups and individuals - especially those who are actively critical of the state, including political opposition members, journalists, and human rights defenders.

The Digital Security Act (DSA), in particular, has led to deeply disturbing implications for both state and non-state actors in the country who are at risk of not only compromising their personal lives but also the integrity of their work. Passed in October 2018 and recently repackaged into and replaced by the Cyber Security Act (CSA), the law cast a tightening noose around freedom of expression, right to privacy and human rights in general by effectively granting multiple law enforcement agencies in the country the overarching authority to accuse, arrest and sentence anyone found posting online content that "ruins communal harmony or creates instability or disorder or disturbs... law and order."[29] The consequences are clear since the passing of this law, newspaper editors only publish 10 to 20 percent of the news reported, out of which 50% of it is self-censored.[30] Abusive provisions such as this, along with complimentary technologies, have found citizens in two extremes: best case scenarios can involve individuals being tracked online for "anti-state" content and subsequently arrested, whilst also having their posts, comments and social media accounts banned or deleted. Worst case scenarios, on the other hand, can mean people being abducted out of their houses late at night with no trace left behind.

---

[28] Samira Hussain, 'His memories uncovered a secret jail - right next to an international airport,' BBC, 16 April 2025, https://www.bbc.com/news/articles/cly6lp567r8o (accessed on 1 September 2025)

[29] Julia Bleckner, 'After the Monsoon Revolution: A Roadmap to Lasting Security Sector Reform in Bangladesh,' 27 January 2025, https://www.hrw.org/report/2025/01/27/after-monsoon-revolution/roadmap-lasting-security-sector-reform-bangladesh (accessed on 1 September 2025)

[30] Human Rights Watch, 'Bangladesh: Online Surveillance, Control,' Human Rights Watch, 8 January 2020, https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control (accessed on 1 September 2025)

According to a report published by Transparency International Bangladesh (TIB), between 2018 and 2023, over 7,000 cases have been filed across the country under the DSA[31], a number which has only steeply increased since then, alongside growing accusations of surveillance amongst citizens and professionals. In February 2021 alone, 4 media personnels, including a writer (Mushtaq Ahmed), cartoonist (Ahmed Kabir Kishore), with 11 others, were arrested and charged by the RAB under DSA, for publishing propaganda, and spreading false/offensive information which was posted on personal social media pages. Most publicly prominent and internationally covered was the arrest of Shafiqul Islam Kajol, a photographer and editor for Pakkhakal Sahfiqual magazine.[32] After over a year of intimidation by intelligence agencies, Kajol was reported missing in March 2020 and was suspected to be a victim of "enforced disappearances"[33] - a suspicion that was categorically denied by law enforcement. Shortly after, a case was registered against Kajol for posting allegedly critical, defamatory, and false content against the government on his personal Facebook page. It was only in December, after much international civil society pressure, that he was released. Employees at Prothom Alo, a leading national newspaper, have faced comparable allegations for publishing content deemed as "tarnishing the image of the nation."[34]

Students and citizens also found themselves victims of the draconian law. In July 2020, a student from Jagannath University, 17-year-old Khadijatul Kubra was arrested for hosting a Facebook webinar where critiques were made against the government by Bangladeshis living abroad. Similarly, countless other students, regardless of where they're residing, have faced similar, sometimes identical charges for having political discussions on social media.[35]

---

[31] Transparency International Bangladesh, 'Digital Security Act 2018 and the draft Cyber Security Act 2023: A Comparative Analysis,' Transparency International Bangladesh, 30 August 2023, https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf (accessed on 1 September 2025)

[32] IFJ, 'Bangladesh: Three journalists charged under Digital Security Act,' International Federation of Journalists, 11 February 2021, https://www.ifj.org/media-centre/news/detail/article/bangladesh-three-journalists-charged-under-digital-security-act (accessed on 1 September 2025)

[33] Amnesty International, 'Bangladesh: Reveal whereabouts of disappeared journalist, end repression,' Amnesty International, 18 March 2020, https://www.amnesty.org/en/latest/news/2020/03/bangladesh-must-reveal-whereabouts-of-disappeared-journalist-and-end-repression/ (accessed on 1 September 2025)

[34] HRW, 'Bangladesh: End Crackdown Against Journalists and Critics,' Human Rights Watch, 3 May 2023, https://www.hrw.org/news/2023/05/03/bangladesh-end-crackdown-against-journalists-and-critics (accessed on 1 September 2025)

[35] Zyma Islam & Emrul Hasan Bappi, 'Digital security act: Sued at 17, JnU student in jail,' The Daily Star, 18 September 2022, https://www.thedailystar.net/news/bangladesh/crime-justice/news/digital-security-act-minor-sued-adult-2yrs-ago-languishing-jail-3121741 (accessed on 1 September 2025)

Such instances are not isolated to the DSA - over the past half-decade, state and non-state actors alike have blamed the Bangladeshi government officials for spying on them and their digital devices. Most recently, the leader of BNP Mirza Fakhrul Islam Alamgir publicly accused the government of using Pegasus to hack into smartphones of political opponents and collect sensitive personal data, including messages, call logs, and documents, in an undemocratic attempt to quell dissent.[36] Shortly thereafter, investigative journalists at WIRED detailed how the NTMC has been involved in collecting and recording individuals' cell phone data and internet activity - all of which was found published onto an unsecure database linked with their systems.[37] According to security experts who found the leak, the agency's database was hacked by anonymous people on the internet, and it was most likely the result of a misconfiguration. More concerning is the nature of the data leak. Cyber security researchers have found that the data found was expressly metadata, including indexes such as "sms," "birth registration," "finance personal details," and "Twitter," as well as IMEI numbers, a unique cellphone identifier that can allow virtually anyone with access to track and clone a device.

Evidence of digital surveillance and tracking citizens have also been reported by members of the Bangladeshi government. In a report by the Commission of Inquiry on Enforced Disappearance published in December 2024, members of the judiciary stated that their investigation into the enforced disappearances of journalists and human rights defenders found "mobile surveillance systems [in use] pinpointing the location of victims" prior to them being picked up by intelligence forces.[38] The document further detailed how officers from the RAB and DGIF confirmed in interviews that "unobtrusive abductions were virtually impossible without mobile surveillance."

This long trail of statements, arrests, leaks, and suspicious alleged abductions has left many individuals suspicious of the state and conscious of how much access and oversight the government has over extrajudicial tracking of individuals' online activity, including posts, comments, videos, livestreams, and articles being shared on not only public forums but also private, personal accounts.

---

[36] 'Fakhrul: Govt hacking smartphones using Pegasus Spyware,' Dhaka Tribune, 8 July 2023, https://www.dhakatribune.com/bangladesh/politics/319943/fakhrul-govt-hacking-smartphones-using-pegasus (accessed on 1 September 2025)

[37] Matt Burgess, 'A Spy Agency Leaked People's Data Online - Then the Data Was Stolen,' WIRED, 16 November 2023, https://www.wired.com/story/ntmc-bangladesh-database-leak/ (accessed on 1 September 2025)

[38] BSS, 'Commission: Mobile surveillance used in pinpointing victims' location,' Dhaka Tribune, 22 December 2024, https://www.dhakatribune.com/bangladesh/368862/commission-mobile-surveillance-used-in (accessed on 1 September 2025)

Surveillance Tools and Systems Used in Bangladesh

Our investigation found that at least 160 surveillance technologies and other spyware systems were imported to and/or deployed in Bangladesh between 2015 and 2025. These tools ranged from IMSI catchers and Wi-Fi interceptors to spyware such as Pegasus, FinFisher, Cellebrite UFED, and Predator, acquired at an aggregate cost of an estimated USD 184.5 million, from France, Germany, the United States, Israel, Canada, the United Kingdom, and often routed through countries like Cyprus, Singapore, and Hungary.[39] Specifically, the NTMC alone appears to have spent over USD 100 million on surveillance technologies, including deep packet inspection (DPI) and decryption platforms to intercept internet traffic, and filter content and extract data. The following section offers a non-exhaustive list of technologies acquired by state agencies in Bangladesh.

Intrusive Spyware for Device Surveillance

The DGFI's use of FinFisher, a spyware suite sold by the British Gamma Group, was confirmed in a report by Citizen Lab.[40] FinFisher is capable of infiltrating targets' computers or phones, enabling full remote access to microphones, cameras, and files. The presence of a FinFisher server on a DGFI network segment in 2015 strongly indicates operational use. Additionally, the Bangladeshi government has reportedly been linked to NSO Group's Pegasus spyware. Pegasus is an advanced tool developed in Israel that can covertly infect smartphones and extract data or turn on cameras/mics without user knowledge. Media reports from 2021 based on the Pegasus Project leaks also suggested that Bangladeshi individuals (including possibly opposition figures or journalists) were targets of Pegasus, although the government "denied buying it."[41] Notably, the government has officially distanced itself from Pegasus, and no conclusive evidence of a direct purchase has emerged.

---

[39] Tech Global Institute, 'The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh,' Tech Global Institute, August 2025, https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf (accessed on 1 September 2025)

[40] Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto & Sarah McKune, 'Pay No Attention to the Server Behind the Proxy,' The Citizen Lab, 15 October 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ (accessed on 1 September 2025)

[41] Star Report, 'Pegasus Spyware: Bangladesh among infected locations,' The Daily Star, 20 July 2021, https://www.thedailystar.net/news/bangladesh/news/pegasus-spyware-bangladesh-among-infected-locations-2134181 (accessed on 1 September 2025)

Integrated Lawful Interception System (ILIS)

The NTMC reportedly deploys a lawful interception system integrated with telecommunication networks in the country. In 2015, according to a New Age report, six mobile operators in Bangladesh collectively paid approximately €20.1million to upgrade the NTMC's functions, enabling direct recording of thousands of live mobile conversations.[42] The German firm Trovicor—which had taken over Nokia Siemens's surveillance equipment business in 2009—supplied the new kit to ensure compatibility with emerging 3G networks. Former Secretary General of the Association of Mobile Telecom Operators of Bangladesh, Nurul Kabir, also confirmed that the mobile phone operators had to pay for the surveillance system as it was "part of their license conditions".[43]Clause 25 of the 4G license agreement, for instance, obligates mobile network operators to enable real-time access to user information, bulk data interception, and live database monitoring by security agencies like the NTMC. Enforcement occurs not only through the threat of criminal prosecution and financial penalties, but also via coercive administrative measures, including the non-renewal of licenses and the withholding of permits.[44] Separately, the NTMC also procured both stationary and vehicle-mounted mobile and data interception systems, with companies like Mobileum, Inc., Yaana Technologies, and Toru Group involved in training of security personnel.[45] In addition, the Bangladesh Telecommunication Regulatory Commission (BTRC) has leveraged Deep Packet Inspection (DPI) technology as part of internet monitoring. DPI is an advanced form of network surveillance that examines the content of data packets in real time, enabling filtering of traffic and extraction of information. While experts note that the same DPI tools used for censorship can be used to surveil users' online activities, in 2019, the government reportedly mandated that all internet service providers install DPI equipment.[46]

---

[42] David Bergman, 'Phone operators pay for govt's surveillance system upgrade,' New Age, 15 February 2015, https://web.archive.org/web/20190531190259/https://archive.newagebd.net/95380/phone-operators-pay-for-govts-surveillance-system-upgrade/ (accessed on 1 September 2025)

[43] Ibid.

[44] Faisal Mahmud, 'Bangladesh ramps up efforts to monitor social media after months of student-led agitations,' Scroll, 21 August 2018, https://scroll.in/article/891011/bangladesh-ramps-up-efforts-to-monitor-social-media-after-months-of-student-led-agitations (accessed on 1 September 2025)

[45] Tech Global Institute, 'The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh,' Tech Global Institute, August 2025, https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf (accessed on 1 September 2025)

[46] Human Rights Watch, 'Bangladesh: Online Surveillance, Control,' Human Rights Watch, 8 January 2020, https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control (accessed on 1 September 2025)

Before the 2024 election, the government was reportedly set to deploy a mobile phone surveillance system - Integrated Lawful Interception System (ILIS) - that would empower law enforcement and intelligence agencies to track users' exact locations and access sensitive personal information. According to the reports, this new surveillance system was obtained at an estimated cost of USD 51.7 million, capable of linking all internet service providers (ISPs), international internet gateways, national internet exchange service providers, and mobile operators to the system of a government agency.[47] Government procurement documents show that the NTMC officials have frequently traveled abroad to procure and train on interception systems. For example, on two separately reported occasions, multiple state officials were sent to the United States to take part in ILIS procurement-related training and technical discussions.[48] The government has been considering its acquisition for a long time. President Abdul Hamid publicly acknowledged its implementation to enable data and voice interception as early as 2018, and reiterated this position in 2023.

[47] Rajib Ahmed, 'Government to launch advanced surveillance system before elections,' Prothom Alo, 18 October 2023, https://en.prothomalo.com/bangladesh/474qjv8eh7 (accessed on 1 September 2025)

[48] Public Security Division, Ministry of Home Affairs, Government of the People's Republic of Bangladesh, 2017, https://mhapsd.gov.bd/ (accessed on 1 September 2025)
Privacy International, 'Updated - Amid Crackdown in Bangladesh, Government forces Continue Spytech Shopping Spree,' Privacy International, 14 August 2018, https://privacyinternational.org/long-read/2226/updated-amid-crackdown-bangladesh-government-forces-continue-spytech-shopping-spree (accessed on1 September 2025)

Mobile Phone Surveillance and IMSI Catchers

An IMSI catcher (also known as a Stingray) is a device which mimics a cell tower, forcibly connecting nearby mobile phones through it and thereby allowing operators to capture device identifiers (like IMSI numbers), track locations, and intercept calls and text messages. Reports from Privacy International have documented how, as early as 2014, the RAB has attempted to procure a vehicle-mounted IMSI catcher, and has continued a "shopping spree" for such tools in subsequent years.[49] Moreover, in early 2021, the Al Jazeera Investigative Unit revealed that in 2018, Bangladesh's DGFI acquired a mobile surveillance system called 'P6 Intercept' - an IMSI catcher system capable of monitoring hundreds of mobile phones simultaneously - manufactured by an Israeli company named PicSix.[50] According to the report, as Bangladesh has no formal diplomatic ties with Israel, this procurement was covert, with the equipment being routed through a company controlled by a Bangkok-based Irish businessman, and the paperwork falsely listing the origin as Hungary. Similarly, an investigation conducted by Haaretz in 2023 found that a 'SpearHead' mobile interception system was shipped to Bangladesh in June 2022. SpearHead, developed by Passitora (owned by a former Israeli intelligence officer and operating out of the Balkans), is a high-end surveillance van outfitted with equipment that can harvest data from all phones within a 1km radius, intercepting calls, messages, and even WhatsApp or Facebook chats.[51] Additionally, Prelysis has reportedly also sold a Wi-Fi interception system to Bangladesh's intelligence in 2019.[52] Our investigation also shows that the RAB and Bangladesh Police appear to have invested in GSM/UMTS vehicular active support systems (i.e. vehicle-mounted IMSI catchers). Equally noteworthy here are reports from Al Jazeera's I-Unit that found , officials from the Public Security Division and RAB were authorized by the government to travel to various countries in the European Union, including the UK, Netherlands and Turkey, for training programs that provide foreign intelligence know-how to conduct mass surveillance.[53]

---

[49] Privacy International, 'Updated - Amid Crackdown in Bangladesh, Government forces Continue Spytech Shopping Spree,' Privacy International, 14 August 2018, https://privacyinternational.org/long-read/2226/updated-amid-crackdown-bangladesh-government-forces-continue-spytech-shopping-spree (accessed on1 September 2025)

[50] Al Jazeera Investigative Unit, 'Bangladesh bought mass spying equipment from Israeli company,' Al Jazeera, 2021, https://www.ajiunit.com/article/bangladesh-bought-mass-spying-equipment-from-israeli-company/ (accessed on 1 September 2025)

[51] 'Israeli spyware and surveillance tools sold to Bangladesh - report,' Jerusalem Post, 10 January 2023, https://web.archive.org/web/20250306114513/https://m.jpost.com/business-and-innovation/tech-and-start-ups/article-728100 (accessed on 1 September 2025)

[52] Oded Yaron & Zulkarnain Saer Khan, 'Bangladesh: Report reveals government purchase of Israeli spy tech; inc. co. comment,' Business & Human Rights Resource Centre, 10 January 2023, https://www.business-humanrights.org/en/latest-news/bangladesh-report-reveals-government-purchase-of-israeli-spy-tech-inc-co-comment/ (accessed on 1 September 2025)

[53] Zulkarnain Saer Khan, Yarno Ritzen & Kevin Hirten, 'Bangladesh's RAB received foreign intelligence training in the EU,' Al Jazeera, 8 December 2022, https://www.aljazeera.com/news/2022/12/8/bangladeshs-rab-received-foreign-intelligence-training-in-the-eu (accessed on 1 September 2025)

Social Media Monitoring and Online Content Surveillance

In recent years, the Bangladeshi government has turned its attention to surveillance of social media and online content, given the growing importance of digital platforms in political discourse. In 2018, the NTMC announced plans to procure a 'Social Media Monitoring System (Open Source Intelligence) and related services' at a cost of BDT 236 crore (approx €25 million).[54] This system was intended to scan and analyze public content on Facebook, X (formerly Twitter), YouTube and other platforms to identify "rumors" or subversive speech. While details of this system and its deployment are scarce, the very issuance of such a tender underscores a dangerous appetite for monitoring of online speech, especially when used to critique or dissent against the government. These moves coincided with the passage of the Digital Security Act 2018, which created offenses for online speech and empowered a new agency to monitor and restrict digital content. By late 2019, the Department of Telecommunication (DoT) had implemented a nationwide system enabling real-time filtering of online content. According to official statements reported in The Daily Star, "the government is now equipped to monitor, block or filter online content, including those on social media."[55] Under a project named 'Cyber Threat Detection and Response', specialized equipment was installed and handed over to the BTRC to run operations. However, the technical features of the technology or their operational uses are not publicly available.

[54] Deepak Acharjee, 'Social media to come under surveillance,' The Independent, 12 June 2018, https://theindependentbd.com/post/153852 (accessed on 1 September 2025)

[55] Muhammad Zahidul Islam, 'Govt can now filter online contents,' The Daily Star, 20 September 2019, https://www.thedailystar.net/frontpage/bangladesh-govt-can-now-monitor-block-filter-online-facebook-contents-1802497 (accessed on 1 September 2025)

Digital Forensic Tools

Alongside surveillance of communications in transit, Bangladeshi authorities have also obtained tools to extract data from devices after seizure. For example, according to Haaretz's report, Cellebrite—an Israeli company known for phone cracking technology—reportedly sold its equipment to Bangladesh's RAB in 2021.[56] Cellebrite's Universal Forensic Extraction Devices (UFED) can reportedly bypass locks and encryption on mobile phones and retrieve call logs, deleted messages, location history, application data, multimedia files, and more. Such technology could be used when security forces detain individuals and confiscate their phones or computers, allowing retrospective surveillance of personal data - even in cases where the crimes they're suspected of are independent of cyberspace. Additionally, official documents show that the Bangladesh e-Government Computer Incident Response Team also sought to procure the UFED Physical Analyzer, which enables more granular analysis, recovery of deleted content, and generation of detailed forensic reports.

This collection of tools illustrates how Bangladesh has steadily built a "surveillance state" apparatus with both breadth (population-level or network-level monitoring) and depth (targeted intrusion into personal devices).

[56] Jerusalem Post, 'Israeli spyware and surveillance tools sold to Bangladesh - report,' Jerusalem Post, 10 January 2023, https://web.archive.org/web/20250306114513/https://m.jpost.com/business-and-innovation/tech-and-start-ups/article-728100 (accessed on 1 September 2025)

Import-Export Data and Trade Pattern in Surveillance Tech

Bangladesh's procurement of cyber surveillance tools has often involved transnational transactions, given that most of this technology is produced abroad. Publicly available trade information and investigative reporting shed light on how these tools are imported:

Bangladesh's lack of formal relations with Israel means direct purchases from Israeli companies are officially prohibited, resulting in largely confidential imports via third or proxy countries. Despite this, multiple Israeli-origin systems have reportedly ended up in Bangladesh, facilitated by third-party countries like Cyprus, Singapore, and Hungary. Export records from Cypriot authorities documented shipments of surveillance systems to Bangladesh in 2019 and 2022, including the Passitora SpearHead van. Similarly, Prelysis and U-TX Technologies also routed their sales through Cyprus, using the island as a go-between to ensure compliance with Israeli export regulations.[57] These examples show how surveillance trade is conducted through complex logistics to bypass political barriers and conceal procurement information, raising transparency concerns. Some imports, on the other hand, have been more straightforward. The installation of the DPI-based content filtering system was done by a local tech integrator, Tech Valley Solutions, importing hardware from the United States, though details of the purchase, such as the manufacturer or model, have not been disclosed in public records or documents.

For Bangladesh, it appears as though acquiring foreign surveillance technology has been easier than developing indigenous solutions, and while it comes at the cost of dependence on external expertise and potential diplomatic friction, it offers an even greater payout in the form of citizens' privacy.

[57] Ibid.

Legal Framework & Practice

The deployment of advanced spyware and mass interception systems have made a direct impact on the privacy of citizens, their communications, interactions, opinions and movements. Article 43 of Bangladesh's Constitution guarantees the privacy of correspondence and other means of communication, while Article 39 safeguards freedom of speech and the press. These fundamental rights are subject to reasonable restrictions imposed by law on certain qualified grounds, such as state security and public order. Although these rights are enshrined in the constitutional framework, however, in practice, these have been consistently undermined by the country's vast surveillance infrastructure, and the policies and institutional mechanisms that support them.

Bangladesh's legal regime has gradually expanded to authorize surveillance with vague and broad provisions that enable abuse of privacy, dignity and the freedom to profess opinions - either on the government or otherwise. Specifically, section 97A of the Bangladesh Telecommunication Regulation Act 2001 (amended in 2006) contains vague provisions that permit law enforcement and intelligence agencies to 'record or collect information' from telecommunication services in the interest of national security, without meaningful procedural safeguards, likely exceeding the permissible thresholds of reasonableness.[58] Similar provisions are also included in the Telegraph Act, 1885, and the Wireless Telegraphy Act, 1933. Complementing these provisions are equally vague regulatory and licensing frameworks that obligate telecommunication service providers to enable information access, data interception, and real-time monitoring at a network-level.[59] Additionally, Section 144 of the Code of Criminal Procedure, 1898 grants authorities sweeping powers to issue executive monitoring or interception orders to service providers based on subjective assessments of potential threats to public order. Systemically, the structuring of telecommunications infrastructure at the network access level—where operators are required by licensing conditions to maintain connections with and provide data access to intelligence services like the NTMC under strict conditions of secrecy—enables state agencies to surveil citizens, effectively bypassing constitutional and legal safeguards.

---

[58] Human Rights Watch, 'Bangladesh: Online Surveillance, Control,' Human Rights Watch, 8 January 2020, https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control (accessed on 1 September 2025)

[59] Shahzeb Mahmood, 'How Bangladesh has been building a digital police state,' The Daily Star, 12 August 2025, https://www.thedailystar.net/opinion/views/news/how-bangladesh-has-been-building-digital-police-state-3960706 (accessed on 1 September 2025)

This contributes to a pervasive lack of transparency and accountability in the system. As Human Rights Watch pointed out, the use of DPI and other blocking technology in Bangladesh occurred "without a sufficient legal framework to protect rights to privacy, expression, and access to information."[60] In effect, the practice of surveillance in Bangladesh has leapt ahead of the law, and the law is being retrofitted in ways that legitimize invasive monitoring post facto, rather than restraining it.

The insertion of Information and Communication Technology (ICT) Act (2006), which later informed equally problematic sections in Bangladesh's legislative framework, further extended the state's disregard for privacy laws in the country to allow institutions the regulatory bandwidth (or lack thereof) to collect and record information for the purpose of using it against individuals who exercised their right to dissent, opinion and critique. Enacted to 'ostensibly… prevent cybercrimes,'[61] under section 9 the Act openly allows the government to maintain electronic records (also known as electronically surveil) which includes SMS, e-mails, photos, videos, audios and other computer data. More disturbingly, various other sections give government agencies the authority and power to intercept any information transmitted through electronic devices, "for the interest of the sovereignty, integrity, or security of Bangladesh."[62] While not directly linked or associated with conventional surveillance as we understand it, it's evident that the ICT Act (2006) and its subsequent amendments in 2013, were introduced at a crucial moment when technology advancements were making it easier for people to voice their concerns without fear. The Digital Services Act (2018), has only added to this existing legal arsenal for this glaring upheaval of citizen rights. Borrowing extensively from the ICT Act, both laws were introduced at a time of extreme democratic turmoil when dissent was on the rise and the need to quell it even higher. Using overly broad and vague provisions, the DSA gave the government enormous and absolute power to record online activity and act upon it to initiate investigations into people accused of being a threat to the state.

---

[60] Human Rights Watch, 'Bangladesh: Online Surveillance, Control,' Human Rights Watch, 8 January 2020, https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control (accessed on 1 September 2025)

[61] Rebecca Mammen John, 'The Information and Communication Technology Act of 2006: Bangladesh's Zombie Cyber Security Law,' Clooney Foundation for Justice & Centre for Governance Studies, November 2024, https://cfj.org/wp-content/uploads/2024/11/Bangladesh-ICT-Act-Report_November-2024-1.pdf (accessed on 1 September 2025)

[62] Zubair Kasem Khan & Dilruba Parvin, 'E-Surveillance Vis-a-Vis Digital Privacy Rights under the Information and Communication Technology (ICT) Act - 2006: Inquesting of New Hope or Hype?' International Journal of Ethics in Social Sciences, 3(2), December 2015, https://www.crimbbd.org/wp-content/uploads/2016/05/3.2.6.pdf (accessed on 1 September 2025)

Other sections further along give increasingly draconian abilities to government officials such as the being able to arrest suspected individuals, confiscate and seize personal devices without need of a warrant, and blocking data or information online based on arbitrary needs.[63] After pushbacks from local and international human rights communities, the DSA was eventually "reconstructed" into the Cyber Security Act (CSA) in 2023; a reconstruction that remains substantially similar to the DSA save for the replacement of words. Interestingly, a new incorporation to the CSA has been an expansion of its territorial reach, including persons beyond the state of Bangladesh if committed within the country's borders.[64]

Simultaneously, there is also no dedicated data protection law in force. While a draft is under consideration, it contains sweeping exemptions for law enforcement and intelligence activities that would allow wide-ranging, unchecked surveillance of citizens' personal data.[65] If, instead, such exemptions were narrowly framed as exceptions—justifiable only on demonstrable grounds of public interest, subject to human rights due diligence, and overseen by an independent body—the risk of their misuse for abusive surveillance could be significantly reduced. However, a rearticulation of the exemption alone would be insufficient; meaningful safeguards would also require complementary mechanisms such as a robust freedom of information framework to ensure transparency, effective institutional checks on executive authority, proactive and independent human rights due diligence and auditing of surveillance practices, and responsive measures to address and sanction unlawful conduct.

---

[63] Ali Riaz, 'How Bangladesh's Digital Security Act Is Creating a Culture of Fear,' Carnegie Endowment for International Peace, 9 December 2021, https://carnegieendowment.org/research/2021/12/how-bangladeshs-digital-security-act-is-creating-a-culture-of-fear?lang=en (accessed on 1 September 2025)

[64] International Center for Non-Profit Law, 'Handbook: Bangladesh's Cyber Security Act: A Guide for Civil Society, Media and the Public,' International Center for Non-Profit Law, October 2024, https://www.icnl.org/wp-content/uploads/Bangladesh-CSA-Handbook-Nov-2024.pdf (accessed on 1 September 2025)

[65] 'Haaretz reports Dhaka bought spy tech from Israeli supplier,' The Daily Star, 11 January 2023, https://www.thedailystar.net/news/bangladesh/news/haaretz-reports-dhaka-bought-spy-tech-israeli-supplier-3217746 (accessed on 1 September 2025)

Case Laws and Precedents

Alongside provisions provided in Bangladesh's legislative frameworks, courts and judiciary have now and then taken up a stance on the importance of privacy rights for its citizens - not only in the context of physical privacy of the person or home but especially digital privacy. Constitutional protections were upheld and reaffirmed in The State and Ors vs. Oli and Ors (2019), a case that succinctly expresses the importance of privacy, especially when administering evidence in an ongoing investigation.[66] Heard in the Supreme Court of Bangladesh in 2019, when prosecution members submitted phone records and call logs obtained from suspicious sources, the authenticity and admissibility of such "legal evidence" was called into question. Under the issue of right to privacy, the court stated that obtaining personal information such as communications records either from public or private avenues (including telecommunications companies) without formal request, seizure, or authoritization, is a violation of constitutional rights.

More specifically in the context of surveillance, is Aynunnahar vs Bangladesh (2016), a case where judges observed that "the right to privacy is an essential foundation of the freedom of dissent... this right cannot be undermined in the name of surveillance."[67] Similar cases as far back as the late 90s with Imtiazur Rahman Farooqui vs. Bureau of Anti-Corruption (1998), solidified how information on correspondence and communication is intrinsic to citizen's privacy. Although the case was particular to facts involving client confidentiality amongst lawyers, experts agree that its precedent can be applied to broader issues of privacy in the country.[68]

While Bangladesh's legal landscape explicitly carves out provisions that aim to protect the privacy and dignity of citizens, with the exception of such case laws, little has been done to ensure implementation and discourage blatant violation, especially by state institutions who either evoke vague national security issues or undertake covert operations where they never have a need to give a reason at all.

---

[66] The State and Ors vs. Oli and Ors (2019), LEX/BDHC/0128/2019

[67] Tech Global Institute, 'A Chipped Tooth: Right to Privacy in the Internet era in Bangladesh,' Tech Global Institute, https://techglobalinstitute.com/announcements/blog/a-chipped-tooth-right-to-privacy-in-the-internet-era-in-bangladesh/ (accessed on 1 September 2025)

[68] Toriqul Islam, 'An assessment of privacy regime in Bangladesh: A legal analysis,' UUM Journal of Legal Studies, 13(2), 21 July 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4194284 (accessed on 1 September 2025)

Recommendations

Oversight and Accountability: A hallmark of Bangladesh's surveillance landscape is the near-total lack of independent oversight. All major law enforcement and intelligence agencies report to the Home Ministry, but their work is shrouded in secrecy, and often protected by official secrecy laws. Without oversight, the public has no way to know the extent of surveillance against them or to seek redress for this invasion of privacy when misused for partisan goals. Law enforcement agencies must be held accountable for conducting surveillance activities. One way to strengthen accountability would be the creation of a statutory parliamentary oversight body with adequate resources and independence. Such a committee should have the authority to review the full range of surveillance activities, demand information and documents, conduct audits and investigations into possible rights violations, and issue public reports. It should also be able to propose legislative changes and refer cases to the judiciary, ensuring both transparency and democratic control.

Judicial Role: To enhance the capacities of courts to provide the necessary checks and balances in this context, a few steps can be taken. The Bangladesh Telecommunications Regulation Act, 2001 needs to be amended to require all interception orders to be approved by a judge (or designated tribunal), based on probable cause, limited to serious criminal investigations, and subject to strict tests of legality, necessity, and proportionality. This process should be time-bound, require detailed justifications, and allow for adversarial review where appropriate. Prior judicial scrutiny would ensure that surveillance is necessary and proportionate to a legitimate security objective. A specialized, quasi-judicial body composed of retired judges, legal scholars, and civil-liberties experts empowered to review, approve, and periodically audit interception requests should be established. There must be accessible avenues for individuals or advocacy groups to challenge the legality of interception orders in a timely manner, with courts empowered to quash unlawful authorizations and award remedies. For the judiciary to discharge its functions effectively, it requires a clear statutory mandate, coupled with institutional independence, adequate technical expertise, and access to impartial expert input, enabling it to evaluate complex surveillance technologies and safeguard their conformity with constitutional and legal boundaries.

The Role of International Actors: The international market for surveillance technology plays a crucial role in enabling current practices in Bangladesh and highlights the need for stricter export controls and greater corporate accountability in the global surveillance industry. Accountability and oversight extend beyond Bangladesh to exporting states, where regional and international frameworks—such as the Wassenaar Arrangement, the Pall Mall Process, and the EU's Dual-Use Regulation—set out principles for responsible transfer and use of surveillance and dual-use tools. Although varying in enforceability, these instruments establish a common human rights baseline and are recognized by many key exporting and intermediary countries. They also provide important avenues for civil society, digital rights groups, and legislators in those jurisdictions to press for greater scrutiny and to question whether such technologies should be supplied to governments with poor human rights records.

Conclusion

Bangladesh's decade-long engagement with cyber intrusion illustrates a fraught nexus of technological capability, state security prerogatives, and individual rights in a nascent democracy. This scoping study has demonstrated that, under the banners of counter-terrorism, national security, and public order, Bangladeshi authorities have deployed an array of intrusive tools—from device-level spyware to national monitoring centres and mobile-data sweeps—sourced through opaque international procurement channels. Collectively, the qualitative evidence—from leaked procurement documents to human-rights investigations—reveals systematic overreach: journalists, political opponents, and civil society actors have been subject to pervasive surveillance, contravening constitutional guarantees of privacy and Bangladesh's obligations under international human rights law. Although lawful interception remains a legitimate function of the modern state, the absence of judicial warrants, transparent authorizations, and meaningful oversight has rendered "lawful" surveillance in Bangladesh indistinguishable from arbitrary state intrusion.

Policy reforms are imperative. First, the government should publish clear disclosures regarding which agencies conduct surveillance, under what legal authorities, and with what technical capabilities. Second, an independent parliamentary and judicial oversight body must be empowered to review, and where appropriate invalidate, surveillance orders. Third, the forthcoming Personal Data Protection Ordinance should be amended to eliminate blanket exemptions for security agencies, mandating court-issued warrants, time-limited data retention, and special protections for journalists, lawyers, and political actors. At this critical juncture, Bangladesh must choose between the entrenchment of digital authoritarianism and the realization of its digital transformation vision grounded in participatory governance. Without decisive legal and institutional safeguards, the current surveillance architecture risks perpetuating a culture of secrecy and mistrust, undermining both individual liberties and the social contract that underpins democratic resilience.

Works Cited

“ARTICLE 19 condemns surveillance through controversial technology.” Dhaka Tribune, January 17, 2023, https://www.dhakatribune.com/bangladesh/302955/article-19-condemns-surveillance-throug

“BTRC blocks Skype.” The Daily Star, November 19, 2018, https://www.thedailystar.net/js-polls-2018/btrc-blocks-skype-1662676

“Communication surveillance versus right to privacy: Where do our laws stand?” The Daily Star, November 24, 2023, https://www.thedailystar.net/opinion/views/news/communication-surveillance-versus-right-privacy-where-do-our-laws-stand-3535416

“Fakhrul: Govt hacking smartphones using Pegasus Spyware.” Dhaka Tribune, July 8, 2023, https://www.dhakatribune.com/bangladesh/politics/319943/fakhrul-govt-hacking-smartphones-using-pegasus

“Govt probes purchase of surveillance equipment during Hasina govt.” New Age, August 14, 2025, https://www.newagebd.net/post/country/273010/govt-to-probe-purchase-of-spy-equipment-during-hasina-govt

“Haaretz reports Dhaka bought spy tech from Israeli supplier.” The Daily Star, January 11, 2023, https://www.thedailystar.net/news/bangladesh/news/haaretz-reports-dhaka-bought-spy-tech-israeli-supplier-3217746

“Israeli spyware and surveillance tools sold to Bangladesh – report.” The Jerusalem Post, January 10, 2023, https://web.archive.org/web/20250306114513/https://m.jpost.com/business-and-innovation/tech-and-start-ups/article-728100

“Mobile service disrupted as BNP rallies at Golapbagh.” The Financial News, December 10, 2022, https://bdnews24.com/bangladesh/k655gvskx3

“NTMC will soon be able to block anti-govt propaganda.” The Daily Star, February 20, 2019, https://www.thedailystar.net/city/online-anti-govt-propaganda-in-bangladesh-ntmc-filter-1704910

"Over 7,000 cases under DSA: Law Minister." The Daily Star, June 5, 2023, https://www.thedailystar.net/news/bangladesh/crime-justice/news/over-7000-cases-under-dsa-law-minister-3338511

"Social media to come under telecom monitoring surveillance." New Age, June 13, 2018, https://www.newagebd.net/article/43598/social-media-to-come-telecom-monitoring-surveillance

Abrahams, Fred. "Judge, Jury and Death: Torture and Extrajudicial Killings by Bangladesh's Elite Security Force." Human Rights Watch, June 6, 2006, https://www.hrw.org/reports/2006/bangladesh1206/bangladesh1206.htm

Abrar, C R. "Machinations of a fearsome state." The Daily Star, January 1, 2017, https://www.thedailystar.net/supplements/unpacking-2017/machinations-fearsome-state-1513066

Acharjee, Deepak. "Social media to come under surveillance." The Independent, June 12, 2018, https://web.archive.org/web/20180613180511/https://www.theindependentbd.com/post/153852

Ahmed, Rajib. "Govt to launch advanced surveillance system before elections." Prothom Alo, October 18, 2023, https://en.prothomalo.com/bangladesh/474qjv8eh7

Al Jazeera Investigative Unit. "All the Prime Minister's Men." Al Jazeera, 2021, https://www.ajiunit.com/investigation/all-the-prime-ministers-men/

Al Jazeera Investigative Unit. "Bangladesh bought mass spying equipment from Israeli company." Al Jazeera, February 2, 2021, https://www.aljazeera.com/news/2021/2/2/bangladesh-bought-surveillance-equipment-from-israeli-company

Amnesty International, "Bangladesh: Reveal whereabouts of disappeared journalist, end repression." Amnesty International, March 18, 2020, https://www.amnesty.org/en/latest/news/2020/03/bangladesh-must-reveal-whereabouts-of-disappeared-journalist-and-end-repression/

Bergman, David. "No Place for Criticism Bangladesh Crackdown on Social Media Commentary." Human Rights Watch, May 9, 2018, www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary

Bergman, David. “Phone operators pay for govt’s surveillance system upgrade.” New Age, February 15, 2015, https://web.archive.org/web/20190531190259/https://archive.newagebd.net/95380/phone-operators-pay-for-govts-surveillance-system-upgrade/

Bleckner, Julia. “After the Monsoon Revolution: A Roadmap to Lasting Security Sector Reform in Bangladesh.” Human Rights Watch, January 27, 2025, https://www.hrw.org/report/2025/01/27/after-monsoon-revolution/roadmap-lasting-security-sector-reform-bangladesh

BSS. “Commission: Mobile surveillance used in pinpointing victims’ location.” Dhaka Tribune, December 22, 2024, https://www.dhakatribune.com/bangladesh/368862/commission-mobile-surveillance-used-in

Burgess, Matt. “A Spy Agency Leaked People’s Data Online - Then the Data Was Stolen.” WIRED, November 16, 2023, https://www.wired.com/story/ntmc-bangladesh-database-leak/

Clarke, Ryan, and Shafqat Munir. “Avoiding Suicide Terrorism in Bangladesh - Combating Terrorism Center at West Point.” Combating Terrorism Center at West Point, May 15, 2009, https://ctc.westpoint.edu/avoiding-suicide-terrorism-in-bangladesh/

Crisis Group. “Beyond the Election: Overcoming Bangladesh’s Political Deadlock” Crisis Group, January 4, 2024, https://www.crisisgroup.org/asia/south-asia/bangladesh/336-beyond-election-overcoming-bangladeshs-political-deadlock

Crisis Group. “Political Conflict, Extremism and Criminal Justice in Bangladesh.” Crisis Group, 2016, https://crisisgroup.org/sites/default/files/277-political-conflict-extremism-and-criminal-justice-in-bangladesh.pdf

FE Online. (2022, Dec 10). Mobile service disrupted as BNP rallies at Golapbagh. The Financial Express. https://thefinancialexpress.com.bd/national/mobile-service-disrupted-as-bnp-rallies-at-golapbagh-1670654249

Ganguly, Sumit. (2006). “The Rise of Islamist Militancy in Bangladesh.” United States Institute of Peace, 2006, https://www.files.ethz.ch/isn/39241/2006_august_sr171.pdf

Hasan, Mubashar. “Democracy and Political Islam in Bangladesh.” South Asia Research, 31, no. 2 (2011): 97–117. https://doi.org/10.1177/026272801103100201

Hossain, Zakir. “INTELLIGENCE AND NATIONAL SECURITY: BANGLADESH PERSPECTIVE.” The Indian Journal of Political Science, 78, no. 3 (2017): 431–441. https://www.jstor.org/stable/26535023

HRW. “Bangladesh: Crackdown as Elections Loom.” Human Rights Watch, December 14, 2018, https://www.hrw.org/news/2018/12/13/bangladesh-crackdown-elections-loom

HRW. “Bangladesh: Crackdown on Social Media.” Human Rights Watch, October 19, 2018, https://www.hrw.org/news/2018/10/19/bangladesh-crackdown-social-media

Human Rights Watch. “Bangladesh: Online surveillance, control.” Human Rights Watch, January 8, 2020, https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control

Hussain, Samira. “His memories uncovered a secret jail - right next to an international airport.” BBC, April 16, 2025, https://www.bbc.com/news/articles/cly6lp567r8o

IFJ, “Bangladesh: Three journalists charged under Digital Security Act.” International Federation of Journalists, February 11, 2021, https://www.ifj.org/media-centre/news/detail/article/bangladesh-three-journalists-charged-under-digital-security-act

International Center for Non-Profit Law, “Handbook: Bangladesh’s Cyber Security Act: A Guide for Civil Society, Media and the Public,” International Center for Non-Profit Law, October 2024, https://www.icnl.org/wp-content/uploads/Bangladesh-CSA-Handbook-Nov-2024.pdf

Islam, Muhammad Zahidul, “Govt can now filter online contents.” The Daily Star, September 20, 2019, https://www.thedailystar.net/frontpage/bangladesh-govt-can-now-monitor-block-filter-online-facebook-contents-1802497

Islam, Toriqul. “An assessment of privacy regime in Bangladesh: A legal analysis.” UUM Journal of Legal Studies, 13, no. 2 (2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4194284

Islam, Zyma, and Emrul Hasan Bappi. “Digital security act: Sued at 17, JnU student in jail.” The Daily Star, September 18, 2022, https://www.thedailystar.net/news/bangladesh/crime-justice/news/digital-security-act-minor-sued-adult-2yrs-ago-languishing-jail-3121741

Jackman, David. “Dominating Dhaka.” Effective States and Inclusive Development, Working Paper No. 127, November 2019, The University of Manchester

John, Rebecca Mammen. “The Information and Communication Technology Act of 2006: Bangladesh's Zombie Cyber Security Law.” Clooney Foundation for Justice & Centre for Governance Studies, November 2024, https://cfj.org/wp-content/uploads/2024/11/Bangladesh-ICT-Act-Report_November-2024-1.pdf

Khan, Zubair Kasem, and Dilruba Parvin. “E-Surveillance Vis-a-Vis Digital Privacy Rights under the Information and Communication Technology (ICT) Act - 2006: Inquesting of New Hope or Hype?” International Journal of Ethics in Social Sciences, 3, no. 2 (2015): 77-88, https://www.crimbbd.org/wp-content/uploads/2016/05/3.2.6.pdf

Khan, Zulkarnain Saer, Yarno Ritzen & Kevin Hirten. “Bangladesh’s RAB received foreign intelligence training in the EU.” Al Jazeera, December 8, 2022, https://www.aljazeera.com/news/2022/12/8/bangladeshs-rab-received-foreign-intelligence-training-in-the-eu

Mahmood, Shahzeb. “How Bangladesh Has Been Building a Digital Police State.” The Daily Star, August 12, 2025, https://www.thedailystar.net/opinion/views/news/how-bangladesh-has-been-building-digital-police-state-3960706

Mahmud, Faisal. “Bangladesh ramps up efforts to monitor social media after months of student-led agitations.” Scroll, August 21, 2018, https://scroll.in/article/891011/bangladesh-ramps-up-efforts-to-monitor-social-media-after-months-of-student-led-agitations

Marczak, Bill, John Scott-Railton, Adam Senft, B. Abdul Razzak, Sarah McKune, and Ron Deibert. “Hide and seek: Tracking NSO Group’s Pegasus spyware to operations in 45 countries.” The Citizen Lab, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Marczak, Bill, John Scott-Railton, Adam Senft, B. Abdul Razzak, Sarah McKune, and Ron Deibert. “Hide and seek: Tracking NSO Group’s Pegasus spyware to operations in 45 countries.” The Citizen Lab, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. “Pay no attention to the server behind the proxy: Mapping FinFisher’s continuing proliferation.” The Citizen Lab, October 15, 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

OHCHR. “Fact Finding: Human Rights Violations and Abuses related to the Protests of July and August 2024 in Bangladesh.” Office of the High Commissioner for Human Rights, February 12, 2025, https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf

Privacy International. “Updated - Amid crackdown in Bangladesh, government forces continue spytech shopping spree.” Privacy International, August 14, 2018, https://privacyinternational.org/long-read/2226/updated-amid-crackdown-bangladesh-government-forces-continue-spytech-shopping-spree

Public Security Division. (2017). Ministry of Home Affairs, Government of the People's Republic of Bangladesh. https://mhapsd.gov.bd/

Riaz, Ali. “How Bangladesh’s Digital Security Act Is Creating a Culture of Fear,” Carnegie Endowment for International Peace, December 9, 2021, https://carnegieendowment.org/research/2021/12/how-bangladeshs-digital-security-act-is-creating-a-culture-of-fear?lang=en

Riaz, Ali. Bangladesh: A Political History Since Independence. I.B. Tauris. 2016

Star Report. “Pegasus spyware: Bangladesh among infected locations.” The Daily Star, July 20, 2021, https://www.thedailystar.net/news/bangladesh/news/pegasus-spyware-bangladesh-among-infected-locations-2134181

Tech Global Institute, “A Chipped Tooth: Right to Privacy in the Internet era in Bangladesh,” Tech Global Institute, https://techglobalinstitute.com/announcements/blog/a-chipped-tooth-right-to-privacy-in-the-internet-era-in-bangladesh/

Tech Global Institute. “The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh.” Tech Global Institute, August 2025, https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf

Thapa, Tejshree. ““The Fear Never Leaves Me”: Torture, Custodial Deaths, and Unfair Trials after the 2009 Mutiny of the Bangladesh Rifles.” Human Rights Watch, July 4, 2012, https://www.hrw.org/report/2012/07/04/fear-never-leaves-me/torture-custodial-deaths-and-unfair-trials-after-2009-mutiny

Transparency International Bangladesh. “Digital Security Act 2018 and the draft Cyber Security Act 2023: A Comparative Analysis.” Transparency International Bangladesh, August 30, 2023, https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf

Uddin, Jamal. (2017, November 29). “Dhaka city set for facial recognition cameras to pinpoint criminals.” Dhaka Tribune, November 29, 2017, https://www.dhakatribune.com/bangladesh/dhaka/131818/dhaka-city-set-for-facial-recognition-cameras-to

United Nations. “Bangladesh: UN report finds brutal, systematic repression of protests, calls for justice for serious rights violations.” United Nations Bangladesh, 2025, https://bangladesh.un.org/en/289108-bangladesh-un-report-finds-brutal-systematic-repression-protests-calls-justice-serious

United States Department of State, ‘Country Reports on Terrorism 2007,’ United States Department of State, April 2008, https://2009-2017.state.gov/documents/organization/105904.pdf

Yaron, Oded, and Zulkarnain Saer Khan. “Bangladesh: Report reveals government purchase of Israeli spy tech; inc. co. comment.’ Business & Human Rights Resource Centre, January 10, 2023, https://www.business-humanrights.org/en/latest-news/bangladesh-report-reveals-government-purchase-of-israeli-spy-tech-inc-co-comment/

INDIA

Chapter 3

DRF USA

Abbreviations

UPA	United Progressive Alliance
CMS	Central Monitoring System
NATGRID	National Intelligence Grid
NETRA	Network Traffic Analysis
CCTNS	Crime and Criminal Tracking Network & Systems
NDA	National Democratic Alliance
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) 20
HRDs	Human Rights Defenders
CERT-In	Indian Computer Emergency Response Team
YSRCP	YSR Congress Party
WB	West Bengal
CM	Chief Minister

TDP	Telugu Desam Party
BJP	Bharatiya Janata Party
JD(U)	Janata Dal (United)
INC	Indian National Congress
JD(S)	Janata Dal (Secular)
NCP	Nationalist Congress Party
DGIPR	Director-General of Information and Publicity
PIL	Public interest litigation
AITC	All India Trinamool Congress
IT Act	Information Technology Act
Information Technology Rules 2009	Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
VPN	Virtual Private Network

DPDP Act	Digital Personal Data Protection Act
OTT	Over the Top
UIDAI	Unique Identification Authority of India
PUCL	People's Union for Civil Liberties

Introduction

India, South Asia's largest country, has developed a sophisticated surveillance system shaped by its colonial legacy and compounded by legal ambiguities. Despite the scale of these capabilities, there is little institutional or constitutional oversight. The Indian government has remained largely silent on the extent and use of surveillance technologies, even amid credible reports of the deployment of NSO Group's controversial Pegasus spyware. Such tools have been used to monitor journalists, activists, and political opponents, undermining democratic accountability. Under the broad and opaque justification of "national security," India's surveillance apparatus has become deeply entrenched within state institutions, posing a growing threat to citizens' fundamental constitutional rights.

Historical Context

India's surveillance architecture is rooted in its colonial past, shaped by the Indian Telegraph Act 1885. Born from British "informational anxiety", especially after the 1857 rebellion, the Act transformed communication into a tool of state dominance, embedding surveillance as a mechanism of control over the 'native' population.[1] It legitimised emergency powers, allowing interception and restriction of communications—not just in crises but as a permanent condition of governance.[2]

Despite decolonisation, constitutional advancements and the proliferation of digital technologies, the underlying logic of surveillance as a means of dominance and control remains intact and may even have expanded as a result. The continuity of control through cyber intrusion in contemporary India underscores the enduring tension between security and civil liberties despite constitutional protections in the state's electoral democracy.

With the increase in internet connectivity in the early 2000s, India's surveillance capabilities expanded significantly with a state apparatus that created legal regulations to keep a closer watch on its citizens.[3] The 2019 Pulwama attack further reinforced the government's call for enhanced monitoring in conflict zones.[4]

---

[1] Christopher Alan Bayly, 'Empire and Information: Intelligence Gathering and Social Communication in India, 1780–1870,' Cambridge University Press. 1996
Deep Kanta Lahiri Choudhry & Kenneth A. Loparo, 'Telegraphic Imperialism: Crisis and Panic in the Indian Empire, c.1830–1920,' Palgrave Macmillan, 2010
Deep Kanta Lahiri Choudhry, '"1857" and the communication crisis,' In S. Bhattacharya (Ed.), Rethinking 1857, Orient Longman, 2007

[2] Giorgio Agamben, 'State of Exception,' University of Chicago Press, 2005
John Reynolds, 'Empire, Emergency and International Law,' Cambridge University Press, 2017
Johannes Thumfart, 'Digital Rights and the State of Exception: Internet Shutdowns from the Perspective of Just Securitization Theory,' Journal of Global Security Studies, 9(1), March 2024, https://doi.org/10.1093/jogss/ogad024 (accessed on 1 September 2025)
Merrin Muhammad Ashraf, 'Unraveling the Digital State of Exception in India,' Law School Policy Review, 6 July 2023, https://lawschoolpolicyreview.com/2023/07/06/unraveling-the-digital-state-of-exception-in-india/ (accessed on 1 September 2025)

[3] P. Arun, 'Power to Intercept, Monitor and Surveil: Cybersurveillance and Democracy in India,' National Law School Journal, 13(1), 1 July 2015, https://repository.nls.ac.in/nlsj/vol13/iss1/5 (accessed on 1 September 2025)

[4] ET Online, 'Pulwama terror attack: What happened on Feb 14 and how India responded, The Economic Times, 14 February 2020, https://economictimes.indiatimes.com/news/defence/pulwama-terror-attack-what-happened-on-feb-14-and-how-india-responded/articleshow/74128489.cms (accessed on 1 September 2025)

Notably, these expansions had not been limited to counterterrorism; events such as communal riots[5] and the COVID-19 pandemic had also been used as justifications for greater state control over digital communications. It is worth noting that the Information Technology Act, 2000 (IT Act)—India's first legislation governing electronic commerce–while not initially intended to, was layered onto the existing colonial-era Telegraph Act, maintaining the state's authority over communications. Such surveillance powers were considerably strengthened following the 2008 Mumbai attacks (26/11).[6]

The Information Technology (Amendment) Act, 2008 (IT Act)[7] granted the government broad monitoring capabilities[8] under section 69 which authorised the state to intercept, monitor and decrypt digital communications on grounds of national security and public order, while Sections 69A and 69B permit website blocking and network traffic monitoring, respectively.

In addition to acquiring targeted surveillance capabilities, the appetite to acquire mass surveillance capabilities also grew from 2010 onwards. Under the United Progressive Alliance (UPA) government (2004–2014), large-scale surveillance infrastructure was introduced, embedding monitoring within governance structures. Key initiatives included:

- Central Monitoring System (CMS): Approved in 2009, operational by 2013, CMS grants the government direct access to telecom networks for real-time monitoring, bypassing service providers.

- National Intelligence Grid (NATGRID): Proposed after 26/11, NATGRID integrates databases from banking, travel, telecom, and immigration sectors for intelligence access.[2]

- Network Traffic Analysis (NETRA): Launched in 2013 by the Defence Research and Development Organisation, NETRA monitors online traffic for flagged keywords, facilitating mass surveillance.

---

[5] Paul R. Brass, 'Development of an Institutionalised Riot System in Meerut City, 1961 to 1982,' Economic and Political Weekly, 39(44), 5 November 2004, http://www.jstor.org/stable/4415744 (accessed on 1 September 2025)

[6] Saroj Kumar Rath, 'New Terror Architecture in South Asia: 26/11 Mumbai Attacks Inquiry,' India Quarterly, 66(4), 359–378, 28 January 2011, https://doi.org/10.1177/097492841006600403 (acccessed on 1 September 2025)

[7] Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

[8] Apar Gupta, 'Balancing Online Privacy in India,' Indian Journal of Law and Technology, 6(1), 2010, https://doi.org/10.55496/AULB6542 (accessed on 1 September 2025)

- Aadhaar: Made available to the public as far back as 2010, this government initiative under the Ministry of Electronics and Information Technology,m provided Indians with unique identification numbers and linked them to multiple public welfare systems.

- Crime and Criminal Tracking Network & Systems (CCTNS): A nationwide database linking thousands of police stations for criminal profiling and tracking.[9]

By 2014, reports indicated that the Union Government (also called the central government - that is, the executive branch of the federal government) alone issued over 100,000 telephone interception orders annually, excluding surveillance conducted at the state level.[10]

Despite the scale of these operations, oversight mechanisms remained weak, with no independent judicial or parliamentary review. Successive governments expanded surveillance capacities, albeit with differing approaches. The UPA embedded surveillance within governance structures through initiatives such as CMS, NATGRID, and Aadhaar, with minimal public debate.[11] From 2014 onwards, the National Democratic Alliance (NDA) government, while continuing these projects, further intensified surveillance.[12]

---

[9] P. Arun, 'Uncertainty and Insecurity in Privacyless India: A Despotic Push towards Digitalisation,' Surveillance and Society, 15(4), 2017, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/6618/6433/15757 (accessed on 1 September 2025)

[10] Press Trust of India, 'Centre taps over 1 lakh phones a yr; many more by states,' Business Standard, 4 September 2014, https://www.business-standard.com/article/pti-stories/centre-taps-over-1-lakh-phones-a-yr-many-more-by-states-114090400673_1.html (accessed on 1 September 2025)

[11] P. Arun, 'Penetrative or Embracive? Exploring State, Surveillance and Democracy in India,' Springer, 27 April 2019, https://doi.org/10.1007/978-981-13-6891-2_11 (accessed on 1 September 2025)

P. Arun, 'In pursuit of personal data: A survey on state surveillance and democracy in India' In P. R. deSouza, M. S. Alam, & H. Ahmed (Eds.), Resilience, fragility, ambivalence (1st ed.). Routledge India, 2021, https://doi.org/10.4324/9781003219477 (accessed on 1 September 2025)

[12] Parul Baxi, 'Technologies of Disintermediation in a Mediated State: Civil Society Organisations and India's Aadhaar Project,' South Asia: Journal of South Asian Studies, 42(3), 554–573, 26 May 2019, https://doi.org/10.1080/00856401.2019.1602808 (accessed on 1 September 2025)

This period (post-2014) matches an overall democratic decline in India, which is marked by a rise of digital authoritarianism in which digital surveillance increased both in qualitative and quantitative intensity. Even after the reaffirmation of privacy as a fundamental right by the Supreme Court in 2017 in K.S. Puttaswamy v. Union of India K.S. Puttaswamy (Privacy-9J.) v. Union of India, 2017 - its status put to question by the Attorney General[13] - the NDA government expanded state monitoring through executive-driven Information Technology (Intermediary Guidelines and Digital Media Ethics Code) (IT Rules), deeper database integration, and legislative enactments that expanded executive control without checks and balances.[14]

The disclosures in 2019 and 2021 concerning the use of Pegasus spyware—a sophisticated surveillance tool developed by the Israeli cyber-intelligence firm NSO Group—marked a critical moment in debates on surveillance in India. These revelations demonstrated the extent to which state surveillance practices extend beyond the legal framework of "lawful interception."[15] Independent investigations reported that more than 300 individuals were identified as potential targets, among them journalists, human rights activists, lawyers, and opposition leaders.[16]

---

[13] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1, AIR 2017 SC 4161
Press Trust of India & HT Correspondent, 'Right to privacy not a fundamental right: Centre tells Supreme Court' Hindustan Times, 27 July 2017, https://www.hindustantimes.com/india-news/right-to-privacy-not-a-fundamental-right-centre-tells-supreme-court/story-bSlTdZjMiAJOoTEq2gNHPM.html (accessed on 1 September 2025)

[14] Bidisha Chaudhuri, 'Distant, opaque and seamful: Seeing the state through the workings of Aadhaar in India,' Information Technology for Development, 27(1), 37–57, 9 July 2010, https://doi.org/10.1080/02681102.2020.1789037 (accessed on 1 September 2025)
Tanmay Singh, 'India's New Intermediary Guidelines,' Verfassungsblog: On Matters Constitutional, 1 June 2025, https://doi.org/10.17176/20210602-003803-0 (accessed on 1 September 2025)
Rina Chandran, 'Surveillance nation: India spies on world's largest population,' Context News, 20 March 2023, https://www.context.news/surveillance/surveillance-nation-india-spies-on-worlds-largest-population (accessed on 1 September 2025)

[15] Ibid

[16] Seema Chishti, 'WhatsApp confirms: Israeli spyware was used to snoop on Indian journalists, activists,' The Indian Express, 1 November 2019, https://indianexpress.com/article/india/whatsapp-confirms-israeli-spyware-used-snoop-on-indian-journalists-activists-pegasus-facebook-6095296/ (accessed on 1 September 2025)
Soumyarendra Barik, 'Pegasus: 300 of 1,400 users from India, why ruling may re-open tapping debate,' The Indian Express, 23 December 2024, https://indianexpress.com/article/business/whatsapp-pegasus-ruling-us-india-9737575/ (accessed on 1 September 2025)

Subsequent forensic analyses confirmed infections of several devices, strongly indicating state involvement, given NSO Group's policy of licensing its spyware exclusively to government clients. The disclosures did not merely expose instances of surveillance but also highlighted the opaque manner in which such technologies are deployed, often without clear legal accountability or transparent oversight mechanisms. They have therefore intensified broader debates on the erosion of privacy rights, the ambiguities surrounding the state's justification for surveillance, and the tension between national security claims and constitutional freedoms.

The controversy eventually reached the Supreme Court of India, which acknowledged the seriousness of the allegations and initiated a review process that remains pending to date. The Pegasus episode has since become emblematic of the growing concerns about digital authoritarianism, raising pressing questions about the balance between technological capacities of the state and the protection of fundamental rights in democratic societies.

Findings

This chapter explores the documented use of cyber-intrusion technologies in India between 2019 and 2025, a period marked by increasing concerns around digital surveillance, opaque state practices, and the erosion of informational transparency. Given the absence of official data on the procurement, deployment, and authorisation of surveillance tools, the analysis relies primarily on investigative journalism, civil society documentation, and the work of international human rights and cybersecurity organisations. These sources have collectively helped map the nature of the technologies deployed, identify the individuals and groups targeted, and assess the institutional responses—or lack thereof—to allegations of unlawful surveillance.

The Indian State maintains no public register of spyware contracts, tenders, or interception orders. Requests for statistical information under the Right to Information Act have routinely been denied, and legal efforts to compel transparency have been met with resistance.[17] In a notable development preceding the period under review, the Union Government issued an administrative notification empowering Union and State Home Secretaries to order the deletion of surveillance data from state-owned computer systems after a period of six months. This move is widely speculated to have been a response to litigation seeking aggregate data on surveillance authorisations, further highlighting the institutional reluctance to disclose even the most basic metadata related to state surveillance.[18]

In this context of profound informational asymmetry, the chapter pieces together publicly available fragments to reconstruct a timeline of cyber intrusion incidents, focusing on which technologies were reportedly used, against whom, and under what circumstances. Although the opacity of government practices necessarily limits the findings, they reveal clear patterns of targeted surveillance against journalists, human rights defenders, political opposition, and civil society actors. This evidentiary base—however incomplete—offers crucial insight into the informal architecture of digital repression in contemporary India.

---

[17] Centre for Internet and Society, 'State of Cyber Security and Surveillance in India: A review of the legal landscape,' Centre for Internet and Society, 9 April 2019, https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf (accessed on 1 September 2025)

[18] Gayatri Malhotra, 'India's new data protection law: No transparency, no privacy,' Context News, 17 August 2023, https://www.context.news/surveillance/opinion/indias-new-data-protection-law-no-transparency-no-privacy (accessed on 1 September 2025)

Findings on Cyber Intrusion in India

Mapping the Deployment of Spyware

2019 Pegasus Disclosures

The deployment of cyber intrusion technologies in India has illuminated the fragile scaffolding of digital rights protections within the country's democratic framework. In April 2019, The Indian Express first reported that at least 24 Indian journalists, lawyers, and human rights defenders had been targeted through a sophisticated surveillance operation.[19] The revelation came after WhatsApp confirmed to the publication that a number of Indian users had been compromised using Pegasus, a military-grade spyware developed by the Israeli firm NSO Group. WhatsApp declined to disclose the identities or exact number of those targeted but confirmed that alerts had been sent out to affected individuals.[20]

Among those who received the warning from WhatsApp were academics, Dalit rights activists, lawyers, and journalists.[21] The disclosure followed a lawsuit filed by WhatsApp in a U.S. federal court against NSO Group, accusing it of facilitating illegal access to the devices of approximately 1,400 users across four continents (Columbia University, n.d.)[22].

[19] Seema Chishti, 'WhatsApp confirms: Israeli spyware was used to snoop on Indian journalists, activists,' The Indian Express, 1 November 2019, https://indianexpress.com/article/india/whatsapp-confirms-israeli-spyware-used-snoop-on-indian-journalists-activists-pegasus-facebook-6095296/ (accessed on 1 September 2025)

[20] Seema Chishti, & Dipankar Ghose, 'Surveillance via WhatsApp: On snoop target list—Rights lawyers to activists, DU prof to Defence journalist,' The Indian Express, 1 November 2019, https://indianexpress.com/article/india/whatsapp-spyware-pegasus-surveillance-india-targets-6097093/ (accessed on 1 September 2025)

[21] Avi Asher-Schapiro, 'After WhatsApp spyware allegations, Indian journalists demand government transparency' Committee to Protect Journalists, 24 February 2020, https://cpj.org/2020/02/whatsapp-spyware-allegations-indian-journalists-government/ (accessed on 1 September 2025)

[22] WhatsApp Inc. v. NSO Group Technologies Limited, Global Freedom of Expression, 16 July 2020, https://globalfreedomofexpression.columbia.edu/cases/whatsapp-inc-v-nso-group-technologies-limited/ (accessed on 1 September 2025)

The targets, according to the filing, included diplomats, political dissidents, journalists, and senior government officials. The same was subsequently confirmed through forensic analysis by Amnesty International and Citizen Lab, which uncovered a coordinated spyware campaign targeting at least nine human rights defenders in India, including activists, lawyers, academics, and journalists.[23] Between January and October 2019, the targets received personalised spearphishing emails containing malicious links designed to install NetWire, a commercially available spyware. Spearphishing involves sending carefully crafted emails—often impersonating trusted contacts—to deceive recipients into opening links or attachments that deploy malicious software onto their devices.[24]

NSO Group has maintained that its Pegasus software is sold exclusively to government clients and is intended for use in counterterrorism and criminal investigations. However, subsequent investigative reports by HuffPost India and Newslaundry suggested otherwise.[25] Their reporting identified some of the individuals targeted in India, including lawyers involved in the Bhima Koregaon case[26], such as Bela Bhatia and Anand Teltumbde—both of whom have been outspoken critics of state excesses and caste-based discrimination.[27]

Evidence of Pegasus's presence in India predated the lawsuit filed by WhatsApp. Citizen Lab had already flagged India as one of the countries where Pegasus infections had been detected. The lab reported suspected infections associated with 33 of the 36 Pegasus operators it had identified globally.[28] Five of those operators were believed to be focused on Asia, with one—codenamed "Ganges"—linked to India and found to be using politically themed domains to potentially lure targets. The operator was reportedly active between June 2017 and September 2018.

---

[23] Amnesty International, 'India: Human Rights Defenders Targeted by a Coordinated Spyware Operation,' Amnesty International. 15 June 2020, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/ (accessed on 1 September 2025)

[24] Ibid

[25] Prateek Goyal, 'Bela Bhatia, Anand Teltumbde, Shalini Gera among Indians snooped on using Israeli spyware,' Newslaundry, 31 October 2019, https://www.newslaundry.com/2019/10/31/breaking-bela-bhatia-anand-teltumbde-among-indians-snooped-on-using-israeli-spyware (accessed on 1 September 2025)

Sanyukta Dharmadhikari, 'The Indian activists, lawyers snooped on through WhatsApp by Israeli spyware Pegasus,' The News Minute, 31 October 2019, https://www.thenewsminute.com/news/indian-activists-lawyers-snooped-through-whatsapp-israeli-spyware-pegasus-111506 (accessed on 1 September 2025)

[26] This refers to a set of legal proceedings stemming from caste-based tensions during the bicentenary commemoration of the 1818 battle, which Dalit communities regard as a victory over upper-caste Peshwa rule. The violence on January 1, 2018, led to the arrest of 16 activists under the UAPA for alleged Maoist links.

[27] Pavan Dahat, Gopal Sathe & Aman Sethi, 'Bhima Koregaon: Lawyers, activists were among those targeted on WhatsApp by Israeli spyware Pegasus,' HuffPost India, 31 October 2019, https://www.huffpost.com/archive/in/entry/whatsapp-hacking-bhima-koregaon-lawyers-targeted_in_5dba8e9ae4b066da552c5028 (accessed on 1 September 2025)

[28] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, & Ron Deibert, 'Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries (Citizen Lab Research Report No. 113),' The Citizen Lab, 18 September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ (accessed on 1 September 2025)

In April 2020, it was reported that NSO Group had developed a surveillance application aimed at tracking the spread of the COVID-19 virus.[29] Reportedly, NSO Group was "actively pitching surveillance tools to their governments and to others around the world," highlighting the company's strategic pivot to public health surveillance amid the pandemic and raising concerns about the normalisation of invasive technologies under the guise of crisis response.[30]

2021 Pegasus Disclosures

On 18 July 2021, The Wire, in collaboration with an international consortium of journalists under the "Pegasus Project", published findings suggesting that the Israeli surveillance firm NSO Group's spyware, Pegasus, had been deployed to target over 300 verified Indian mobile telephone numbers.[31] Those identified included individuals across a broad spectrum of public life: ministers, opposition leaders, journalists, lawyers, businesspersons, scientists, and human rights activists. The revelations were based on a leaked database obtained by Forbidden Stories, a Paris-based media non-profit, and Amnesty International. While the NSO Group maintains that it licenses its software exclusively to vetted government clients, the breadth of individuals implicated in the leak raised serious concerns about the abuse of surveillance technologies in democratic contexts by States.

[29] Rory Cellan-Jones, 'Coronavirus: Israeli spyware firm pitches to be Covid-19 saviour,' BBC News, 2 April 2020, https://www.bbc.com/news/health-52134452 (accessed on 1 September 2025)

[30] Devdutta Mukhopadhyay, 'Statement: IFF joins international civil society orgs to oppose the NSO Group's attempt to evade responsibility for the Pegasus hack #SaveOurPrivacy,' Internet Freedom Foundation, 24 December 2020, https://internetfreedom.in/ninth-circuit-amici-brief-whatsapp-nso-group-pegasus-hack/ (accessed on 1 September 2025)

[31] Siddharth Varadarajan, 'Pegasus Project: How phones of journalists, ministers, activists may have been used to spy on them,' The Wire, 18 July 2021, https://thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying/ (accessed on 1 September 2025)

Subsequent reporting by The Wire and The Washington Post[32], supported by forensic analyses conducted by Amnesty International's Security Lab, confirmed that Pegasus had been used to compromise at least 37 devices, including those of 10 Indian nationals. Among the Indian targets were journalists and editors with a long record of critical reporting: Sushant Singh (formerly of Indian Express), Paranjoy Guha Thakurta (formerly EPW), S.N.M. Abdi (formerly Outlook), and The Wire's founding editors, Siddharth Varadarajan and M.K. Venu. Although the NSO Group has disclaimed responsibility for the leaked database—stating that it did not constitute a list of Pegasus targets and may have been accessed by clients for unspecified "other purposes"—the forensic confirmation of infections has added weight to claims of illegitimate surveillance.[33]

These developments underscore the opacity of transnational surveillance markets and the absence of meaningful public accountability in the deployment of intrusive digital tools. They also illustrate the risks faced by journalists and civil society actors in contexts where national security rationales are routinely invoked to shield executive conduct from scrutiny.

In January 2022, the New York Times Magazine reported that the Government of India had supposedly procured Pegasus spyware from the Israeli firm NSO Group in July 2017 for the purpose of conducting targeted surveillance.[34] This transaction is understood to have formed part of a broader, opaque arrangement coinciding with high-level diplomatic exchanges—including bilateral visits by Prime Minister Narendra Modi and then Israeli Prime Minister Benjamin Netanyahu.

In March 2023, the Financial Times disclosed that India was actively negotiating new spyware contracts, with values ranging up to 120 million USD.[35] These negotiations reportedly involve firms like the Intellexa Alliance, a group of companies prominently featured in the Predator Files for facilitating the global misuse of spyware.[36]

---

[32] Washington Post, 'Takeaways from The Pegasus Project: forensic analyses show 37 compromised devices, including 10 Indian numbers,' The Washington Post. 2 August 2021, https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/ (accessed on 1 September 2025)

[33] Anuj Srivas, & Kabir Agarwal, 'Snoop list has 40 Indian journalists, forensic tests confirm presence of Pegasus spyware on some,' The Wire, 18 July 2021 https://thewire.in/media/pegasus-project-spyware-indian-journalists/ (accessed on 1 September 2025)

[34] Ronen Bergman, & Mark Mazzetti, 'The Battle for the World's Most Powerful Cyberweapon,' The New York Times Magazine, 28 January 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html (accessed on 1 September 2025)

[35] Mehul Srivastava & Kaye Wiggins, 'India hunts for spyware that rivals controversial Pegasus system,' Financial Times, 31 March 2023, https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9 (accessed on 1 September 2025)

[36] Amnesty International, 'Global: 'Predator Files' spyware scandal reveals brazen targeting of civil society, politicians and officials,' Amnesty International, 9 October 2023, https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/ (accessed on 1 September 2025)

Apple Threat Notifications

On 30 October 2023, Apple Inc. issued threat notifications to a group of Indian opposition leaders, journalists, and researchers, alerting them that "state-sponsored attackers may be targeting your iPhone."[37] These alerts are part of Apple's global threat notification protocol, introduced after the Pegasus spyware revelations in 2021, and are issued when credible threat intelligence indicates that a user is being individually targeted due to their identity or public role.[38] According to Apple, such attacks are highly sophisticated, expensive, and evolve rapidly, making them exceptionally difficult to detect.[39] While the company acknowledges the possibility of false positives, it has confirmed that such notifications are not issued lightly and should be treated as serious indicators of attempted surveillance.

Notably, forensic analyses following Apple's threat notifications in other jurisdictions have confirmed successful infections. In October 2023, Apple's alerts to Russian journalists, including the publisher of Meduza, were validated by Citizen Lab and Access Now.[40] Amnesty International's Security Lab has likewise confirmed Pegasus infections following Apple alerts in countries including India, Serbia, Jordan, and Armenia. While a threat notification does not confirm device compromise, it signals a credible attempt to do so—and, in multiple cases, has led to the verification of spyware intrusions through forensic testing.[41]

---

[37] 'Apple warns top Indian opposition leaders, journalists about 'state-sponsored' attack on phone, The Wire, 31 October 2023, https://thewire.in/rights/apple-india-state-sponsored-spyware (accessed on 1 September 2025)

[38] Amnesty International, 'Apple threat notifications: What they mean and what you can do,' Amnesty International, 11 April 2024, https://www.amnesty.org/en/latest/news/2024/04/global-apple-threat-notifications-what-they-mean-and-what-you-can-do/ (accessed on 1 September 2025)

[39] Apple Inc., 'About Apple threat notifications and protecting against mercenary spyware,' Apple Support, 25 April 2025, https://support.apple.com/en-in/102174 (accessed on 1 September 2025)

[40] Access Now, 'Hacking Meduza: Pegasus spyware used to target Putin's critic,' Access Now, 13 September 2023, https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/ (accessed on 1 September 2025)

[41] Amnesty International, 'Global/India: Apple notifications highlight the unabated threat of unlawful targeted surveillance,' Amnesty International. 31 October 2023, https://www.amnesty.org/en/latest/news/2023/10/global-india-apple-notifications-highlight-the-unabated-threat-of-unlawful-targeted-surveillance/ (accessed on 1 September 2025)
Amnesty International, 'India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists,' Amnesty International, 28 December 2023, https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/ (accessed on 1 September 2025)

Victims of Spyware

Significant revelations regarding the scope and deployment of cyber intrusion technologies have come not through domestic mechanisms, but through litigation and investigative efforts abroad. In WhatsApp Inc. v. NSO Group Technologies, a case that recently resulted in a historic ruling that found the Israeli firm in violation of federal and state law[42] WhatsApp disclosed that India had the second-highest number of Pegasus victims globally, trailing only Mexico.[43] The company reported that approximately 120 Indian users had been targeted with the spyware since 2019.

Investigations conducted by Amnesty International and Citizen Lab independently corroborated a coordinated Pegasus campaign directed at Indian human rights defenders (HRDs).[44] WhatsApp's breach notifications confirmed that over 100 individuals globally—including more than 20 Indian lawyers, activists, and academics—had been targeted. Among them were individuals actively involved in advocacy linked to the Bhima Koregaon case, including lawyers Nihalsing B. Rathod, Degree Prasad Chouhan, and Yug Mohit Choudhary; activist Ragini Ahuja; and academics Partho Sarothi Ray and P.K. Vijayan.[45]

Among the political class, several prominent opposition leaders were allegedly targeted, including Rahul Gandhi, senior leader of the Indian National Congress; G. Parameshwara, then Deputy Chief Minister of Karnataka; H. D. Kumaraswamy, former Chief Minister of Karnataka; and Siddaramaiah, another former Chief Minister and senior Congress figure. Ashok Lavasa, a former Election Commissioner known for dissenting against the Election Commission's exoneration of Prime Minister Modi during the 2019 elections, was also believed to have been on the list. Notably, Ashwini Vaishnaw, the current Minister for Electronics and Information Technology, who assumed office just weeks before the Pegasus revelations surfaced, was also named, though he issued a strong denial in Parliament. His inclusion, if confirmed, would signal the breadth and arbitrariness of targeting.

---

[42] Access Now, 'Statement on WhatsApp v. NSO case,' Access Now, 10 January 2025 https://www.accessnow.org/press-release/statement-on-whatsapp-v-nso-case-decision/ (accessed on 1 September 2025)

[43] Lorenzo Franceschi-Bicchierai, 'Court document reveals locations of WhatsApp victims targeted by NSO spyware,' TechCrunch, 9 April 2025, https://techcrunch.com/2025/04/09/court-document-reveals-locations-of-whatsapp-victims-targeted-by-nso-spyware/ (accessed on 1 September 2025)

[44] Amnesty International, 'India: Human Rights Defenders Targeted by a Coordinated Spyware Operation,' Amnesty International, 15 June 2020, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/ (accessed on 1 September 2025)

[45] Swati Deshpande, 'Seven Elgar accused's phones to be given to Supreme Court Pegasus panel,' Times of India, 9 February 2022, https://timesofindia.indiatimes.com/city/mumbai/7-elgar-accuseds-phones-to-be-given-to-sc-pegasus-panel/articleshow/89439466.cms (accessed on 1 September 2025)

Special Correspondent, 'New online platform maps Pegasus spread,' The Hindu. 7 July 2021 https://www.thehindu.com/news/national/new-online-platform-maps-pegasus-spread/article35185350.ece (accessed on 1 September 2025)

Perhaps the most disturbing case involved the surveillance of a former Supreme Court staffer who had accused then Chief Justice Ranjan Gogoi of sexual harassment. Phone numbers associated with the woman and her family appeared on the leaked Pegasus list.[46]

As observed by an expert from India on the surveillance landscape in India, victims of spyware are frequently those whom the state constructs as 'the Other,' a term that many in the human rights space have used to refer to commonly marginalized communities. Journalists, lawyers, opposition members, and political dissidents are particularly vulnerable in this regard, as their activities are often perceived as destabilizing to state authority or undermining dominant narratives. By situating such groups outside the boundaries of legitimacy, the state not only legitimizes but also normalizes their surveillance.

Mapping the response of the Union Government

Government of India's Responses to Pegasus Allegations: A Chronological Account

The Indian central government's handling of the Pegasus spyware controversy unfolded over several years and was marked by consistent denial, deflection, and reliance on procedural justifications rather than substantive engagement with the underlying allegations.

November 2019: Parliamentary Evasion

The controversy first surfaced on the floor of Parliament following WhatsApp's disclosure that Pegasus spyware, developed by the Israeli firm NSO Group, had been used to target approximately 1,400 users globally, 121 of whom were Indian. On 20 November 2019, responding to a question by Asaduddin Owaisi[47] in the Lok Sabha, Minister for Electronics and Information Technology Ravi Shankar Prasad declined to address the central question of whether the government had procured or used the spyware. Instead, he characterised media reporting as an attempt to "malign the Government of India" and asserted that adequate provisions existed under the IT Act, 2000 to address hacking and spyware.

---

[46] Ajoy Ashirwad Mahaprashasta, Sukanya Shantha, & Kabir Agarwal, 'Days After Accusing CJI Gogoi of Sexual Harassment, Staffer Put on List of Potential Snoop Targets,' The Wire, 19 July 2021, https://thewire.in/rights/ranjan-gogoi-sexual-harassment-pegasus-spyware (accessed on 1 September 2025)

[47] Ministry of Electronics and Information Technology, 'Lok Sabha: Starred Question No. *47', Government of India, 20 November 2011 https://sansad.in/getFile/loksabhaquestions/annex/172/AS47.pdf?source=pqals (accessed on 1 June 2026)

Eight days later, on 28 November, Prasad appeared before the Rajya Sabha, where questioning was more pointed. He was asked directly by members of the opposition, whether the government had procured Pegasus, the Minister stated only that "no unauthorised interception has been done, to the best of my knowledge".[48] When pressed further on whether any transaction had occurred between the Indian government and NSO Group, the Minister evasively responded by referring to the procedures followed by security agencies and the penalties applicable for violations, without confirming or denying the existence of any such transaction.[49]

On 11 December 2019,[50] a further parliamentary response, this time to an unstarred question in the Lok Sabha by Anumula Revanth Reddy, acknowledged for the first time that the government had in fact been informed by WhatsApp of the vulnerability and of the 121 Indian users potentially affected. Yet even this belated acknowledgment was framed as a vindication rather than a cause for concern. The response reiterated that "these attempts to malign the Government of India for the reported breach are completely misleading. The Government is committed to protect the fundamental rights of citizens, including the right to privacy. The Government operates strictly as per provisions of law and laid down protocols. There are adequate safeguards to ensure that no innocent citizen is harassed or his privacy breached" again without addressing the core question of state involvement.

July 2021: The Monsoon Session and Renewed Controversy

The issue resurfaced with considerably greater intensity in July 2021, when a consortium of international journalists published findings from the Pegasus Project identifying Indian journalists, activists, opposition figures, and constitutional functionaries among potential surveillance targets. The disclosure coincided with the opening day of the Monsoon Session of Parliament, a session that was subsequently disrupted.

---

[48] Damini Nath, 'WhatsApp spying issue: No interception says Ravi Shankar Prasad,' The Hindu, 28 November, 2021, https://www.thehindu.com/news/national/whatsapp-spying-issue-no-interception-says-ravi-shankar-prasad/article61613549.ece (accessed on 1 June 2026)

[49] Manu Sebastian, 'WhatsApp Spyware: Union IT Minister Evades Question In Rajya Sabha On Whether Govt Sought Pegasus Services,' Live Law, 28 November 2019, https://www.livelaw.in/top-stories/whatsapp-spyware-union-it-minister-evades-question-in-rajya-sabha-on-whether-govt-sought-pegasus-services-150258 accessed on 1 June 2026)

[50] Ministry of Electronics and Information Technology, 'Lok Sabha: Unstarred Question No. 3686', Government of India, 11 December 2019, https://sansad.in/getFile/loksabhaquestions/annex/172/AU3686.pdf?source=pqals (accessed on 1 June 2026)

The new Minister for Electronics and Information Technology, Ashwini Vaishnaw, who was himself reportedly identified as a potential target[51], rose in Parliament to dismiss the reporting as a "sensational story" and an "attempt to malign Indian democracy and its well-established institutions".[52] He drew an explicit parallel with the 2019 WhatsApp disclosures, noting that those reports had been denied by all parties, including before the Supreme Court, and suggesting that the new reports were of the same character.

Vaishnaw's statement invoked the established legal framework for surveillance, including the Information Technology Act, 2000, the Indian Telegraph Act, 1885, and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, as evidence that India possessed "well-established procedures for lawful surveillance" sufficient to prevent unauthorised interception. He also raised a technical objection to the methodology of the reportage, noting that the mere presence of a number in a leaked dataset did not establish that the corresponding device had in fact been infected with Pegasus. He further cited NSO Group's position that the spyware was made available only to vetted government clients for lawful purposes.

MeitY's Written Response to the Journalist Consortium

In a formal written response to the consortium of journalists that had broken the Pegasus Project story, MeitY reiterated that India was "a robust democracy committed to ensuring the right to privacy to all its citizens as a fundamental right".[53] The Ministry went further, suggesting that the queries posed reflected "poorly conducted research and lack of due diligence by the esteemed media organizations involved". It also pointed to the government's prior response to a Right to Information application concerning Pegasus as sufficient to rebut the allegations, without specifying what that RTI response contained or how it exculpated the government.[54]

---

[51] Fatima Khan, 'IT minister Vaishnaw, on Pegasus list himself, says illegal snooping impossible in India,' The Print, 19 July 2021, https://theprint.in/india/it-minister-vaishnaw-on-pegasus-list-himself-says-illegal-snooping-impossible-in-india/698923/ (accessed on 1 June 2026)

[52] Ministry of Electronics and IT, 'IT Minister Shri Ashwini Vaishnaw's Statement in Parliament on "Alleged use of spyware Pegasus to compromise phone data of some persons as reported in Media on 18th July 2021"' Press Information Bureau, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1736803&ref=static.internetfreedom.in&reg=48&lang=2 (accessed on 1 June 2026)
Anushka Jain and Tanmay Singh, 'Line-by-line verification of the IT Minister's Statement on the Pegasus Hacks,' Internet Freedom Foundation, 30 July 2021, https://internetfreedom.in/line-by-line-verification-of-the-it-ministers-statement-on-the-pegasus-hacks/ (accessed on 1 June 2026)

[53] ANI (@ANI), 'Government of India's response to inquiries on the 'Pegasus project' media report,' X, 18 July 2021, https://x.com/ANI/status/1416800154871468036

[54] The Federal, 'Centre refers to 2019 RTI response to say it doesn't spy on journos, politicians,' The Federal, 19 July 2021, https://thefederal.com/news/pegasus-project#goog_rewarded (accessed on 1 June 2026)

Parliamentary Committee: A Blocked Inquiry

Attempts at legislative scrutiny were frustrated. The Standing Committee on Information Technology, chaired by Congress MP Shashi Tharoor, sought to convene a meeting to examine the Pegasus allegations.[55] The meeting reportedly collapsed for want of a quorum, with BJP members allegedly declining to register their attendance, thereby preventing the committee from functioning. Civil society organisations had made representations to the committee seeking a formal investigation, but this procedural obstruction foreclosed that avenue.

Apple Threat Notification

When the Apple Threat Notifications were issued, the Government of India, rather than engaging substantively with these revelations, responded with dismissal and deflection.[56] At a press conference held on 31 October 2023, the Minister for Electronics and Information Technology, Ashwini Vaishnaw, described Apple's alerts as a "vague advisory" sent to "150 countries," and denied any government role in surveillance.[57] He invoked a prior Supreme Court directed investigation into Pegasus—whose findings remain undisclosed to date—and asserted that "nothing came out of that". The Minister concluded his remarks by accusing the Opposition of distracting from the government's development agenda, branding them as "compulsive critics."

---

[55] HT Correspondent, 'IT panel meet on Pegasus put off after BJP MPs refuse to take part,' Hindustan Times, 29 July 2021, https://www.hindustantimes.com/india-news/it-panel-meet-on-pegasus-put-off-after-bjp-mps-refuse-to-take-part-101627497289549.html (accessed on 1 June 2026)

[56] Apar Gupta, 'Why government's defence on Apple spyware advisory is weak – and in bad faith,' The Indian Express, 2 November 2023 https://indianexpress.com/article/opinion/columns/apar-gupta-writes-why-governments-defence-on-apple-spyware-advisory-is-weak-and-in-bad-faith-9009581/ (accessed on 1 September 2025)

[57] PTI, 'Govt to probe Oppn MPs' claims of getting hacking attempt warnings from Apple,' Deccan Herald, 31 October 2023, https://www.deccanherald.com/india/govt-orders-probe-after-opposition-mps-claims-of-receiving-hacking-attempt-warnings-from-apple-2749839/ (accessed on 1 September 2025)

Vaishnaw also announced an investigation by the Indian Computer Emergency Response Team (CERT-In), an agency that functions under the same ministry. However, the structure and scope of this inquiry raise serious concerns. CERT-In lacks institutional independence, with appointments and oversight resting under ministerial control. Its mandate is primarily technical, focused on device-level cybersecurity breaches, and does not extend to questions of procurement, authorisation, or executive accountability. The inquiry is thus designed to be procedurally narrow, limited to smartphone forensics, and incapable of addressing the larger constitutional issues raised by the repeated targeting of individuals with spyware. Notably, CERT-In was exempted from the purview of the Right to Information Act, 2005, in November 2023.[58]

The international civil society organisation Access Now, known globally for its cybersecurity support and assistance to victims of targeted digital surveillance, was itself subjected to a misinformation campaign following the Apple threat notifications in India.[59] Members of the ruling establishment suggested—without evidence—that Access Now was somehow behind the alerts. Notably, Sanjeev Sanyal, a member of the Economic Advisory Council to the Prime Minister, publicly questioned the legitimacy of the alerts, asking: "How is this external agency able to send such authentic looking messages through the system?"[60] This statement not only mischaracterises the role of Access Now, which has no involvement in Apple's notification system, but also reflects a broader pattern of delegitimising credible civil society actors who work to uncover surveillance abuses.

---

[58] Vijaita Singh, 'Central government exempts CERT-In from RTI Act,' The Hindu, 25 November 2023, https://www.thehindu.com/news/national/central-government-exempts-cert-in-from-rti-act/article67569804.ece (accessed on 1 September 2025)

[59] Anurag, 'NGO behind Apple's dubious alert message to politicians is funded by Soros and Ford Foundation,' OpIndia, 1 November 2023, https://www.opindia.com/2023/11/access-now-ngo-behind-warning-messages-sent-on-behalf-of-apple-is-funded-by-soros-and-ford-foundation/ (accessed on 1 September 2025)

[60] Sanjeev Sanyal (@sanjeevsanyal) "Very curious indeed. The security threat messages being received by some prominent Apple users is not quite from Apple but from a Soros-linked NGO called http://accessnow.org. How is this external agency able to send such authentic looking messages though the system??" X, 1 November 2023, https://x.com/sanjeevsanyal/status/1719571401546297629

Mapping Responses of State Governments

Politically, state responses to the Pegasus revelations have split along party lines. BJP-ruled States have dismissed the claims or targeted organisations like Amnesty International, whereas opposition-ruled constituents have called for probes or condemned the use of spyware. These divergent positions highlight both the constitutional complexity and the lack of transparency in India's surveillance framework.

State	Political Party in Power (at time of response)	Response to Pegasus Revelations
Andhra Pradesh	YSR Congress Party (YSRCP)	Following allegations by West Bengal (WB) Chief Minister (CM) Mamata Banerjee[61] that the former Telugu Desam Party (TDP) government had acquired Pegasus, the Assembly passed a resolution to set up an inquiry committee. The TDP denied the claim.[62] Former intelligence chief A.B. Venkateswara Rao confirmed that Pegasus offered spyware for purchase and discussions occurred, but said the spyware was rejected as "illegal per se."[63]
Assam	Bharatiya Janata Party (BJP)	CM Himanta Biswa Sarma dismissed the revelations as an "international conspiracy to defame India's democracy and also target Prime Minister Narendra Modi"–calling for a ban on Amnesty International for its role in the Pegasus Project.[64]

[61] TNN, 'Bengal was offered Pegasus for Rs 25 crore 4–5 years ago, says Mamata Banerjee,' Times of India, 18 March 2022, https://timesofindia.indiatimes.com/city/kolkata/mamata-pegasus-was-on-offer-for-25-crore/articleshow/90300716.cms (accessed on 1 September 2025)

[62] MN Samdani, 'Andhra Pradesh: TDP govt didn't buy Pegasus spyware, says N. Chandrababu Naidu,' Times of India, 19 March 2022, https://timesofindia.indiatimes.com/city/amaravati/andhra-pradesh-tdp-govt-didnt-buy-pegasus-spyware-says-n-chandrababu-naidu/articleshow/90314865.cms (accessed on 1 September 2025)

[63] P. Sujatha Varma, 'Pegasus had offered its spyware, but TDP government rejected it, says Lokesh,' The Hindu, 18 March 2022, https://www.thehindu.com/news/national/andhra-pradesh/pegasus-had-offered-its-spyware-but-tdp-government-rejected-it-says-lokesh/article65234861.ece (accessed on 1 September 2025)

[64] Utpal Parashar, 'International conspiracy to defame India': Assam CM on Pegasus row,' Hindustan Times, 20 July 2021, https://www.hindustantimes.com/india-news/international-conspiracy-to-defame-india-assam-cm-on-pegasus-row-101626796355634.html (accessed on 1 September 2025)

Bihar	Janata Dal (United) – JD(U)	CM Nitish Kumar stated that a detailed inquiry was necessary to ascertain the facts surrounding the Pegasus allegations.[65]
Chhattisgarh	Indian National Congress (INC)	CM Bhupesh Baghel called the alleged deployment of Pegasus by the Union Government an "act of treason" (ANI, 2022).[66] A three-member committee was formed in 2019 after reports of Pegasus targeting WhatsApp users in the state.[67] No updates on its findings have been made public.
Haryana	Bharatiya Janata Party (BJP)	CM Manohar Lal Khattar questioned Amnesty International's credibility and alleged it was attempting to tarnish India's image.[68]
Karnataka	BJP (following fall of JD(S)-INC govt in 2019)	The Wire reported Pegasus links to numbers associated with the JD(S)-Congress government.[69] Former CM Siddaramaiah wrote to the President's Secretariat alleging surveillance. The matter was referred to the Ministry of Home Affairs and then to the State Government.[70]

[65] Subhash Pathak, 'Pegasus row: Bihar CM seeks detailed probe into allegations of phone-hacking,' Hindustan Times, 2 August 2021, https://www.hindustantimes.com/cities/patna-news/pegasus-row-bihar-cm-seeks-detailed-probe-into-allegations-of-phone-hacking-101627911806760.html (accessed on 1 September 2025)

[66] ANI, 'Centre purchased 'Pegasus spyware' to commit treason,, says CM Bhupesh Baghel,' ANI, 29 January 2022, https://www.aninews.in/news/national/general-news/centre-purchased-pegasus-spyware-to-commit-treason-says-cm-bhupesh-baghel20220129181753/ (accessed on 1 September 2025)

[67] Dipankar Ghose, 'Chhattisgarh govt sets up panel to probe WhatsApp snoop cloud,' The Indian Express, 11 November 2019, https://indianexpress.com/article/india/chhattisgarh-govt-sets-up-panel-to-probe-whatsapp-snoop-cloud-pegasus-6113600/ (accessed on 1 September 2025)

[68] Hitender Rao, 'Pegasus spyware: Khattar questions Amnesty International's credibility,' Hindustan Times, 21 July 2021 https://www.hindustantimes.com/cities/chandigarh-news/pegasus-spyware-khattar-questions-amnesty-international-s-credibility-101626893867660.html (accessed on 1 September 2025)

[69] Ajoy Ashirwad Mahaprashasta, 'Leaked snoop list suggests surveillance may have played role in toppling of Karnataka govt in 2019,' The Wire, 20 July 2021, https://m.thewire.in/article/politics/karnataka-government-toppling-pegasus-spyware-surveillance (accessed on 1 September 2025)

[70] Express News Service, 'Pegasus snooping: MHA asks Karnataka government to probe Siddaramaiah's complaint,' The Indian Express, 8 November 2021 https://indianexpress.com/article/cities/bangalore/pegasus-snooping-mha-asks-karnataka-government-to-probe-siddaramaiahs-complaint-7612364/ (accessed on 1 September 2025)

Maharashtra	Shiv Sena–INC–NCP coalition	After 2021 disclosures, the government questioned a 2019 visit by five representatives of the director-general of information and publicity (DGIPR) to Israel. A public interest litigation (PIL) before the Bombay High Court alleged the trip was linked to Pegasus procurement.[71]
West Bengal	All India Trinamool Congress (AITC)	A Commission of Inquiry chaired by Justice Madan B. Lokur was set up in July 2021, but was later stayed by the Supreme Court in December 2021.[72] In March 2022, CM Banerjee stated Pegasus was offered to the WB Police for ₹25 crore but was declined.[73]

[71] Omkar Gokhale, 'Bombay HC seeks state DGIPR's response on PIL alleging Pegasus link to 2019 Israel study tour,' The Indian Express, 5 August 2021, https://indianexpress.com/article/cities/mumbai/pil-seeks-maharashtra-government-reply-on-2019-study-tour-to-israel-7440147/ (accessed on 1 September 2025)

[72] Shiv Sahay Singh, 'Pegasus spyware issue: West Bengal govt. sets up two-member inquiry commission,' The Hindu, 27 July 2021 https://www.thehindu.com/news/cities/kolkata/pegasus-spyware-issue-west-bengal-govt-sets-up-two-member-inquiry-commission/article35534671.ece (accessed on 1 September 2025)

[73] HT Correspondent, 'Offered to Bengal for ₹25 crore, didn't buy it: Mamata on Pegasus spying software,' Hindustan Times, 18 March 2022 https://www.hindustantimes.com/india-news/offered-to-bengal-for-rs-25-crore-didn-t-buy-it-mamata-on-pegasus-spying-software-101647544349347.html (accessed on 1 September 2025)

Legal Framework

This section proceeds in two parts. Part I provides an overview of the existing legal framework governing the intersection of privacy, data protection, and surveillance in India. It situates these laws within a broader judicial and constitutional culture that has historically privileged state power over individual rights in the domain of national security and technological regulation. Part II engages with the litigation challenging the deployment and constitutional validity of mercenary spyware Pegasus before the Indian Supreme Court. Commonly referred to as the "Pegasus litigation", these proceedings arose after revelations that journalists, lawyers, and human rights defenders in India were allegedly targeted using the spyware.

The Pegasus revelations did not emerge in isolation. They are situated within a broader legal and institutional context that has, over time, witnessed the consolidation of executive power in matters concerning surveillance, data governance, and individual privacy. This consolidation has occurred through both legislative enactments and executive rule-making. Two statutes in particular are the Digital Personal Data Protection Act, 2023, and the Telecommunications Act, 2023. They were passed with little to no meaningful parliamentary scrutiny. Each statute, in its own way, extends and entrenches the surveillance capacities of the state, while offering minimal procedural safeguards or avenues for individual redress. Compounding these concerns is the position that even evidence obtained through illegal means—such as unauthorised wiretaps—can be admitted in court if it is relevant to the case.[74] This creates perverse incentives for law enforcement to bypass legal safeguards, knowing that unlawfully gathered evidence may still be used. Simultaneously, the executive has exercised its subordinate legislative powers to frame rules and directions that significantly dilute privacy protections. Particularly, the CERT-In Cyber Security Directions of 2022, and the Information Technology Rules of 2021 create a regulatory architecture that is opaque, coercive, and structurally skewed in favour of the state. These developments collectively reflect a shift in the surveillance paradigm from targeted, judicially-sanctioned interception to a regime of generalised, pre-emptive monitoring facilitated by law.

---

[74] Venkatesh Vijayaraghavan, & Sameer Singh, 'Look But Don't Touch: A Critique of the Indian Position on Evidence Illegally Obtained Through Tape Recording,' National Law School of India Review, 12(1), 2000, https://repository.nls.ac.in/nlsir/vol12/iss1/8 (accessed on 1 September 2025)

Information Technology Act, 2000

India's framework for electronic surveillance is primarily grounded in Section 69 of the Information Technology Act, 2000 (IT Act), which empowers the Central and State Governments to intercept, monitor, or decrypt any information transmitted, received, or stored in any computer resource. The grounds for such surveillance are broadly worded, encompassing interests such as the sovereignty and integrity of India, defence, national security, public order, and the investigation of cognisable offences. The procedure to be followed is prescribed under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. However, these Rules have been widely criticised for the absence of independent oversight and for vesting excessive discretion in executive authorities. Notably, there is no requirement for prior judicial authorisation. The constitutional validity of Section 69 and the 2009 Interception Rules remains pending adjudication before the Supreme Court of India.

Unauthorised use of spyware such as Pegasus may attract penal consequences under Section 66, which criminalises unauthorised access to computer resources, "downloads, copies or extracts any data" or "introduces or causes to be introduced any computer contaminant or computer virus".

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The traceability provision under Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, compels platforms to identify the first originator of a message upon government request, effectively dismantling end-to-end encryption.[76] By weakening encryption standards, the provision expands the state's surveillance capabilities while undermining secure communication. This not only erodes individual privacy but also creates a chilling effect on speech, as users may hesitate to engage in open discourse due to the fear of state scrutiny.

[75] John Xavier, 'WhatsApp vs Government | Why exiting India threat bestirs 'traceability' debate,' The Hindu, 27 April 2024 https://www.thehindu.com/sci-tech/technology/whatsapp-vs-government-why-exiting-india-threat-bestirs-traceability-debate/article68113037.ece (accessed on 1 September 2025)

CERT-In Cybersecurity Directives (2022)

In 2022, the Indian Computer Emergency Response Team (CERT-In) issued cybersecurity directives applicable to both businesses and individuals that raised privacy concerns.[76] Key mandates included:

I. Extended Data Retention: VPNs, cloud services, and crypto exchanges must store customer data for five years, severely impacting user anonymity.

II. Mandatory Reporting: Cyber incidents must be reported within six hours, placing heavy compliance burdens on companies.

III. Log Synchronisation: Entities must sync system clocks with government-designated time servers, enabling precise activity tracking.

Issued without public consultation, these directives faced criticism from industry and digital rights groups.[77] Several foreign VPN providers such as ExpressVPN, NordVPN and Surfshark exited India in protest.[78]

---

[76] Ministry of Electronics & IT, 'CERT-In issues directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet,' Press Information Bureau, 28 April 2022, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1820904 (accessed on 1 September 2025)
Siddharth Chaturvedi, & Himanshi Srivastava, 'The constitutionality of the new Indian CERT-In VPN rules,' International Data Privacy Law, 13(4), 24 July 2023 https://doi.org/10.1093/idpl/ipad015 (accessed on 1 September 2025)

[77] Access Now, 'India's CERT-In must withdraw April directions and strengthen privacy and cybersecurity,' Access Now, 1 June 2022 https://www.accessnow.org/press-release/india-cert-in-directions/ (accessed on 1 September 2025)

[78] Varsha Bansal, 'VPN providers flee India as a new data law takes hold,' Wired, 25 September 2022 https://www.wired.com/story/vpn-firms-flee-india-data-collection-law/ (accessed on 1 September 2025)

Digital Personal Data Protection Act, 2023

Enacted after prolonged deliberations, the Digital Personal Data Protection Act, 2023 (DPDP Act) seeks to regulate data processing while recognising privacy rights. However, broad exemptions dilute its efficacy. Section 17 permits the government to exempt agencies from compliance for reasons of national security or public order, enabling unchecked data collection. The DPDP Act legally enables government data-sharing, allowing personal data to be repurposed without fresh consent, effectively legalising NATGRID-like integrations. The DPDP Act suffers from the absence of independent oversight and even amends the Right to Information Act, 2005, increasing state secrecy.

This marks a missed opportunity for meaningful surveillance reform, as it grants broad exemptions to state law enforcement authorities. Notably, the Justice Srikrishna Committee (2017) had explicitly recognised that the lack of inter-branch oversight over executive intelligence functions—such as surveillance—is not merely problematic in practice but, following K.S. Puttaswamy v. Union of India, potentially unconstitutional.[79]

[79] Vrinda Bhandari, & Renuka Sane, 'Protecting citizens from the state post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee report and the Data Protection Bill, 2018,' Socio-Legal Review, 14(2), 11 October 2023, https://ssrn.com/abstract=3251982 (accessed on 1 September 2025)
Gayatri Malhotra, 'Delhi HC issues notice on writ petition seeking extent of e-surveillance carried out by MHA under S 69 of IT Act,' Internet Freedom Foundation, 22 March 2023, https://internetfreedom.in/delhi-hc-issues-notice-on-writ-petition-seeking-extent-of-e-surveillance-carried-out-by-mha-under-s-69-of-it-act/ (accessed on 1 September 2025)

Indian Telecommunications Act, 2023: Re-legislating Colonial Provisions

While the Indian Telecommunications Act, 2023, has been framed as a break from colonial-era legislation, it largely reproduces the regulatory logic of the Indian Telegraph Act, 1885.[80] Rather than dismantling its underlying framework, the new Act reinforces and extends state control over communication networks, including digital platforms and encrypted messaging services such as WhatsApp and Signal. Despite the rhetoric of decolonisation, the Act maintains the core principles of state surveillance and information control that characterised colonial governance.

Key provisions that mirror or expand upon colonial-era controls include:

I. Legal Mandate for Interception: The government retains broad interception powers, akin to Section 5(2) of the Telegraph Act.

II. Regulation of OTT ("Over the Top") Services: Messaging platforms such as WhatsApp and Signal are potentially subject to the same compliance obligations as telecom operators, potentially undermining end-to-end encryption.

III. State Control Over Networks: The government may assume control of telecom services during emergencies, reinforcing its ability to impose internet shutdowns

[80] Ministry of Communications, 'The Telecommunications Act 2023: Ushering in a new era of connectivity,' Press Information Bureau, 5 July 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2031057 (accessed on 1 September 2025)
Apar Gupta, 'Telecom law upgrades for a digital authoritarian state,' The Hindu, 23 December 2023 https://www.thehindu.com/opinion/op-ed/telecom-law-upgrades-for-a-digital-authoritarian-state/article67666811.ece (accessed on 1 September 2025)
Tejasi Panjiar, & Gayatri Malhotra, 'A draft to Surveil: IFF's Analysis of the Draft Telecom Interception Rules, 2024,' Internet Freedom Foundation, 12 September 2024, https://internetfreedom.in/telecom-interception-rules-2024-analysis/ (accessed on 1 September 2025)
SFLC, 'Comments on the Draft Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024,' Software Freedom Law Center, 10 October 2024, https://sflc.in/comments-on-the-draft-telecommunications-procedures-and-safeguards-for-lawful-interception-of-messages-rules-2024/ (accessed on 1 September 2025)

Litigation and Judicial Oversight

India's surveillance framework comprises layers of both antiquated and modern laws that expand state surveillance without transparency or meaningful oversight. Unlike democracies where intelligence agencies operate under legislative scrutiny, India's surveillance agencies remain under executive control. Institutions like UIDAI, NATGRID, and CMS operate with little transparency, blurring the line between governance and surveillance.

The judiciary has played an inconsistent and ineffective role in challenging unchecked surveillance by either proposing safeguards or broad principle-based pronouncements that have failed to provide meaningful reform. These include:

- People's Union for Civil Liberties (PUCL) v. Union of India (2018)[81] established procedural safeguards for phone tapping.

- K.S. Puttaswamy v. Union of India (2017)[82] recognised privacy as a fundamental right, imposing legal limits on data collection.

- The Aadhaar Case: K.S. Puttaswamy (Aadhar-5J.) v. Union of India (2018)[83] restricted the mandatory use of Aadhaar (India's biometric identity programme) for non-essential services, citing privacy concerns.

- Pegasus Case prompted the Supreme Court to scrutinise spyware deployment.

However, enforcement remains inconsistent, and government entities are not held to account. The lack of ex-ante judicial authorisation for surveillance orders weakens these precedents.

[81] People's Union for Civil Liberties (PUCL) vs. Union of India, (2018) 1 SCC 301, 1997 AIR SCW 113

[82] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors, (2017) 10 SCC 1, AIR 2017 SC 4161

[83] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2018) 1 SCC 809

Judicial response to Pegasus revelations

The Pegasus revelations triggered a series of constitutional challenges before the Supreme Court of India, seeking accountability for what is arguably one of the most serious allegations of illegal state surveillance in independent India. The petitions were filed by individuals directly implicated in the disclosures, journalists, activists, and public intellectuals, whose phone numbers appeared in the leaked database accessed by the Pegasus Project. Among them were Jagdeep Chhokar (founder of the civil society group, Association for Democratic Reforms), journalists Paranjoy Guha Thakurta and N. Ram, and Rajya Sabha MP John Brittas.[84] They sought an independent judicial inquiry into whether the Indian government procured and deployed Pegasus, and if so, whether such surveillance met the threshold of legality, necessity, and proportionality as articulated in Puttaswamy (2017).[85]

In addition to seeking accountability, the petitioners placed before the Court the broader constitutional implications of unchecked surveillance: its chilling effect on speech, its corrosive impact on democratic dissent, and its outright violation of the right to privacy. Importantly, they pointed to the government's refusal to either confirm or deny the use of Pegasus.[86]

Among the most significant petitions was that of Rupesh Kumar Singh and Ipsa Shatakshi, activists working on displacement and extra-judicial violence in Adivasi regions.[87] Their petition challenged the constitutional validity of the deployment of invasive spyware like Pegasus and also advanced a critical claim: that the government had failed to discharge its positive obligation under Puttaswamy (2017) to protect citizens from privacy violations, including by third parties or rogue state actors. The use of Pegasus was in direct violation of the IT Act, and the absence of transparency regarding its deployment amounted to a breach of the constitutional "right to know". Without information about the perpetrators, duration, and scope of surveillance, the petitioners argued, meaningful legal redress and democratic accountability were rendered impossible.

---

[84] Vakasha Sachdev, '5 Pegasus victims move SC, decry 'state-sponsored illegal hacking',' The Quint. 2 August 2021 https://www.thequint.com/news/law/paranjoy-guha-thakurta-snm-abdi-prem-shankar-jha-rupesh-kumar-singh-ipsa-shatakshi-say-use-of-spyware-against-them-was-illegal-hacking-not-lawful-surveillance (accessed on 1 September 2025)

[85] Surya Kant J, N.K. Singh J, 'Manohar Lal Sharma v. Prime Minister: Pegasus spyware probe case – Background,' Supreme Court Observer, 16 July 2025, https://www.scobserver.in/cases/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-case-background/ (accessed on 1 September 2025)

[86] Anushka Jain & Krishnesh Bapat, 'In Pegasus battle, the fight for surveillance reform,' The Hindu, 9 December 2022, https://www.thehindu.com/opinion/lead/in-pegasus-battle-the-fight-for-surveillance-reform/article65667538.ece (accessed on 1 September 2025)

[87] Rupesh Kumar & Others v. Union of India & Others, Redacted Writ Petition, Supreme Court of India, July 31, 2021. https://drive.google.com/file/d/1dgXAOtvBrXc6YFUDfB4THu4AKix1RvYE/view

The Pegasus litigation began with a petition by M.L. Sharma, a lawyer with a notorious reputation for filing poorly prepared public interest cases.[88] Seen as "busybody" filings, such petitions are usually dismissed quickly, raising fears that the Pegasus challenge too might be trivialised from the outset. This not only undermines strategic litigation but also jeopardises the legitimate claims of victims, whose serious grievances risk being lost amid weak or frivolous petitions.

Throughout the proceedings, the Union Government adopted a stance of calculated evasion. It repeatedly refused to file a substantive affidavit, ultimately submitting a vague and non-committal response in the form of a "limited affidavit" that merely echoed prior statements made in Parliament.[89] The government's blanket invocation of "national security" was used to avoid addressing the core constitutional claims, reflecting a growing trend where security becomes a rhetorical shield for executive impunity.[90]

On 27 October 2021, in M.L. Sharma v. Union of India (2021)[91], the Supreme Court of India constituted an independent technical committee[92] led by former Supreme Court judge Justice RV Raveendran to investigate whether the Government—Union or State—procured and deployed Pegasus to spy on Indian citizens, and if so, whether such surveillance complied with constitutional safeguards. It was also directed to recommend reforms to surveillance law and grievance mechanisms for unlawful surveillance.

---

[88] Nalini Sharma, 'A peek into ML Sharma's world of publicity interest litigation,' India Today, 23 July 2021 https://www.indiatoday.in/law/story/peek-manohar-lal-sharma-world-public-interest-litigation-1831753-2021-07-23 (accessed on 1 September 2025)

[89] Scroll Staff, 'Pegasus: Centre refuses to file affidavit in SC on surveillance allegations, cites national security,' Scroll, 13 September 2021, https://scroll.in/latest/1005257/pegasus-centre-refuses-to-file-affidavit-in-sc-on-surveillance-allegations-cites-national-security (accessed on 1 September 2025)

[90] Union of India, Limited affidavit on behalf of Union of India, 16 August 2021 https://drive.google.com/file/d/1U1BluslRyS1Qk3awdFf9QUyM1hGeg-gq/view

[91] Manohar Lal Sharma (Pegasus Spyware) v. Union of India, (2023) 11 SCC 401

[92] The Committee comprises Mr. Alok Joshi, IPS, former head of the Research & Analysis Wing, and Dr. Sundeep Oberoi, Chairman of ISO/IEC JTC 1/SC7. The committee further includes three technical experts: Dr. Naveen Kumar Chaudhary, Dean of the School of Cyber Security and Forensics, National Forensic Sciences University, Gandhinagar; Dr. Prabhaharan P., Professor in the School of Engineering, Amrita Vishwa Vidyapeetham, Kerala; and Dr. Ashwin Anil Gumaste, Associate Professor of Computer Science and Engineering, IIT Bombay.

While the Supreme Court's decision to form the committee was a step forward, it stopped short of drawing an adverse inference from the union government's refusal to answer direct questions. Instead of compelling disclosure, the Supreme Court opted for a fact-finding process without first determining whether constitutional obligations had already been breached. In this context, concerns arise about delay and procedural drift, what scholar Gautam Bhatia terms as India's long history of "death by committee" risks turning structural rights violations into footnotes of bureaucratic process.[93]

Incidentally, the Supreme Court also rejected the Union Government's vague national security defence and refusal to file a substantive affidavit. It was observed that mere invocation of "national security" cannot shield executive action from judicial review. The Supreme Court reiterated that all citizens and not just journalists or activists, have a reasonable expectation of privacy, and that surveillance must be lawful, necessary, and proportionate.

More troubling, however, was the Supreme Court's conduct in relation to parallel attempts at investigation.[94] When the State of West Bengal constituted its own committee to probe Pegasus, the Supreme Court entertained a challenge to it, despite no clear legal basis. Through oral observations, it expressed disapproval of the State's initiative, effectively compelling it to disband the inquiry.[95] No reasoned order or legal justification was offered for this intervention. That the Court prevented a State government from investigating potential breaches of fundamental rights—without explanation—raises troubling questions about federalism and the judiciary's own role in enabling opacity.

---

[93] Gautam Bhatia, 'The (Continuing) Doctrine of Judicial Evasion in the Aadhaar Case,' Constitutional Law and Philosophy, 9 May 2017, https://indconlawphil.wordpress.com/2017/05/09/the-continuing-doctrine-of-judicial-evasion-in-the-aadhaar-case/ (accessed on 1 September 2025)

[94] Shristi Ojha, 'BREAKING: Supreme Court stays probe of Justice Lokur Commission constituted by WB Govt in Pegasus case,' Live Law, 17 December 2021 https://www.livelaw.in/top-stories/supreme-court-restrains-justice-lokur-commission-constituted-by-wb-govt-from-probing-pegasus-case-187885 (accessed on 1 September 2025)

[95] Supreme Court Observer. 'Pegasus spyware probe #6: Court refuses to stay activities of West Bengal commission,' Supreme Court Observer, 17 December 2021 https://www.scobserver.in/reports/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-day-6-oral-hearings/ (accessed on 1 September 2025)

Findings of the Technical Committee

On 26 August 2022—over a year after the petitions were filed—the Supreme Court of India opened the report submitted to it in a “sealed cover”, but did not share it with the parties. The Chief Justice stated in open court that the report comprised three parts: two prepared by the Technical Committee and one containing observations by Justice R.V. Raveendran (Retd.). It was disclosed that malware had been found on 5 out of the 29 phones examined, although it was not conclusively identified as Pegasus. The Chief Justice also observed that the Union Government had not cooperated with the Committee. While select portions of the report were read aloud during the hearing, no part of it was annexed to a written order. To date, the report remains sealed and has not been made accessible either to the petitioners, their lawyers, or the public.

As the petitioners sought access to findings related to their own devices, the Committee had requested confidentiality, citing security risks and the privacy concerns of individuals who had submitted their devices. The Chief Justice noted that Part III of the report—the observations by Justice R.V. Raveendran (Retd.)—could be made public, but the formal order only recorded that the entire report would remain sealed with the Secretary General.

In addition to the sealed report and judgement, the Committee recommended amending surveillance laws to reflect the right to privacy; strengthening cybersecurity law; protecting citizens from unlawful surveillance; creating a complaint mechanism; and establishing an independent agency to investigate cyberattacks. However, these recommendations remain unenforceable so long as documents remain sealed. The petitioners still do not know whether their devices were among the five on which malware was detected. Without disclosure of the report, its findings, as well as the testing methodology used, the findings cannot be corroborated or independently verified.

Pegasus Hearings––latest dispatch from 2025

The Pegasus petitions remained unlisted and unheard by the Supreme Court of India for nearly three years, reflecting a now-routine pattern of judicial evasion in cases involving national security and civil liberties. Rather than adjudicating the matter, the Court effectively decides by not deciding, leaving petitioners without meaningful closure or redress. The case was eventually heard in April 2025, after an undue delay, raising serious concerns about procedural lapses and the failure of the Supreme Court to act in a timely manner.

At the most recent hearing on 29 April, 2025 the Supreme Court made several troubling oral observations. Justice Surya Kant remarked: "What is wrong if the country used that spyware for security reasons against anti-national elements? There is nothing wrong with having spyware. Against whom it is used, is the point." He further stated that while individual apprehensions may be addressed, "any report which touches upon the security and sovereignty of the country will not be disclosed... Individuals who want to know whether they are included can be informed, but it cannot be made a document for discussion on the streets." Referring to the recent Pahalgam terror attack, he added: "With the scenario happening now, we have to be careful."[96]

This framing omits the core constitutional question: who is termed as an anti-national element and is the deployment of invasive spyware like Pegasus against Indian citizens legally permissible? The government has consistently refused to confirm or deny its use, invoking national security. Yet, as the Supreme Court reiterated in Madhyamam Broadcasting Limited v. Union of India (2023)[97] procedural fairness cannot be dispensed with solely on that ground.

---

[96] Debby Jain, 'Nothing wrong in country using spyware for security; Question is against whom it's used: Supreme Court in Pegasus case,' Live Law, 29 April 2025 https://www.livelaw.in/top-stories/supreme-court-pegasus-spyware-judicial-probe-into-illegal-surveillance-290684 (accessed on 1 September 2025)
Krishnadas Rajagopal, 'Supreme Court asks what's wrong if country using Pegasus against 'anti-nationals', agrees to examine if private citizens were hacked,' The Hindu, 29 April 2025 https://www.thehindu.com/news/national/pegasus-row-supreme-court-says-wont-disclose-report-that-touches-countrys-security-sovereignty/article69504285.ece (accessed on 1 September 2025)

[97] Madhyamam Broadcasting Limited v. Union of India, 2023 SCC OnLine SC 366

In the absence of public disclosure or judicial scrutiny, affected individuals are left without any meaningful remedy. The continued reliance on sealed covers insulates executive action from accountability and undermines the Court's constitutional role as the guardian of citizens' fundamental rights.

These institutional failures are compounded by the absence of a legislative framework governing surveillance in the digital age. Despite repeated calls—including by the Court in Puttaswamy (2018) and civil society organizations in the country—for reform, there has been no political, legislative or judicial will to enact robust safeguards against arbitrary surveillance.

Equally concerning is the judicial culture that treats national security as a trump card. In sensitive matters, courts often defer reflexively to executive claims, applying the proportionality standard inconsistently or not at all. As several public law scholars have noted,[98] this deference risks hollowing out constitutional rights through the very exceptions meant to protect them.

[98] Chintan Chandrachud, 'India - The Kashmir Internet restrictions - India's Supreme Court swaps seats with the Executive,' Public Law, (4), 1 October 2020, https://search.informit.org/doi/10.3316/agispt.20200917036801 (accessed on 1 September 2025)
Gautam Bhatia, 'Unsealed covers: A decade of the Constitution, the courts and the state,' HarperCollins, 2023

Recommendations

Confronting Unlawful Deployment of Cyber Intrusion Technologies in India: Gaps, Opportunities, and Pathways Forward

India presents a particularly challenging context for addressing the unlawful deployment of spyware. Despite credible revelations—most notably involving Pegasus spyware—there has been no formal admission by the State regarding the use of cyber surveillance technologies. Core democratic institutions, including the judiciary and constitutionally mandated oversight bodies, have largely refrained from initiating meaningful investigations into who is deploying spyware, under what legal authority, against whom, and for what purpose. This institutional inertia is compounded by the absence of a dedicated legal framework: India's surveillance regime continues to rely on colonial-era legislation such as the Indian Telegraph Act, 1885 and the Information Technology Act, 2000, both of which confer broad and opaque powers with minimal safeguards or accountability.

Opportunities for Transnational Accountability

Amid this domestic vacuum, a narrow but critical window for strategic engagement has emerged through transnational channels. Collaborations between Indian civil society and global technology companies—such as WhatsApp and Apple—have created new opportunities for accountability beyond borders. Notably, litigation in foreign jurisdictions, such as WhatsApp v. NSO Group in the United States, demonstrates the potential of cross-border legal action to challenge spyware manufacturers. In a significant outcome, collaboration with local civil society contributed to NSO being ordered to pay $168 million in damages to WhatsApp for the Pegasus spyware hack.[99] However, within India, domestic legal remedies remain slow, inconsistent, and often compromised by executive influence.

[99] Access Now, 'NSO to pay $168 million in damages to WhatsApp for Pegasus spyware hacking,' Access Now, 6 May 2025 https://www.accessnow.org/press-release/whatsapp-v-nso-case-damages-decision/ (accessedon 1 September 2025) Devdutta Mukhopadhyay, 'Statement: IFF joins international civil society orgs to oppose the NSO Group's attempt to evade responsibility for the Pegasus hack #SaveOurPrivacy,' Internet Freedom Foundation, 24 December 2020, https://internetfreedom.in/ninth-circuit-amici-brief-whatsapp-nso-group-pegasus-hack/ (accessed on 1 September 2025)

Building a Resilient Ecosystem Through Capacity Building

Indian civil society has played a crucial role in spotlighting the democratic harms of unlawful surveillance. Yet, efforts are frequently constrained by limited access to technical expertise and the high threshold for evidentiary proof of spyware infections—especially in legal proceedings. Making incorrect or unverified claims can damage years of credibility and strategic advocacy. There is therefore an urgent need to build local capacity in digital forensics, evidentiary standards, and strategic litigation, particularly among lawyers, journalists, human rights defenders, and other vulnerable communities.

Knowledge transfer from civil society organisations in the Global North—many of whom have led high-impact investigative collaborations such as the Pegasus Project—can serve as a vital resource. Simultaneously, technology companies that issue threat notifications, such as Apple and WhatsApp, must be urged to provide transparent, disaggregated data and forensic reports on surveillance alerts. Such disclosures are essential for identifying patterns and formulating effective legal and policy responses.

Systemic capacity building must lie at the heart of any forward-looking strategy. This includes targeted training not only for activists and journalists, but also for legal professionals, including judges and lawyers, to deepen awareness of surveillance law and practices. Civil society organisations should be equipped to lead these training efforts, promoting legal literacy, technical know-how, and cybersecurity hygiene. Over time, such initiatives can cultivate a legally empowered ecosystem capable of mounting sustained challenges to unlawful surveillance and advocating for structural reform.

Engaging in Global Norm-Shaping Forums

India's absence from emerging international norm-setting efforts—such as the Pall Mall Process, which aims to govern the use of cyber intrusion technologies—represents a missed opportunity. Indian civil society should be actively supported to participate in such multilateral forums, offering grounded insights drawn from local surveillance contexts. International partners can play a catalytic role by providing technical and policy support to Indian actors, both to advocate for India's inclusion and to help translate domestic experiences into globally relevant contributions that consolidate Global South efforts in changing the geographical landscape of spyware today.

Civic education campaigns to reframe privacy as a constitutional right and counter prevailing indifference to surveillance in South Asia

Legal and technical reform efforts must be complemented by robust public awareness and advocacy. In South Asia, privacy has often been sidelined in favour of economic or political rights, and is frequently dismissed under society's "nothing to hide" trope. Civic literacy campaigns must therefore seek to re-centre privacy as a constitutional right, highlighting its intersection with dignity, equality, and freedom of expression. By reshaping cultural narratives and educating the public on the systemic implications of unchecked surveillance, civil society can help build the democratic consensus necessary to support meaningful surveillance reform.

Strategic Litigation as a Tool for Structural Change

Finally, strategic litigation remains a powerful mechanism to contest state overreach and push for structural reform of India's surveillance framework. However, such efforts are currently hampered by a scarcity of petitioners and legal professionals with the requisite technical and constitutional expertise. Many potential victims of spyware surveillance—particularly those from marginalised or dissenting communities—fear reprisals or further endangerment. This chilling effect is exacerbated by the unequal availability of legal resources and safe channels of recourse.

Addressing these gaps requires sustained investment in civil society-led capacity building to support victims, develop robust legal strategies, and create protective mechanisms for engagement. Only through a coordinated ecosystem of legal, technical, and civic action can India begin to mount an effective and rights-respecting response to unlawful surveillance.

Conclusion

India's surveillance architecture reveals a deep continuity between colonial logics of control and contemporary mechanisms of digital governance. Despite constitutional guarantees and judicial recognition of privacy as a fundamental right, the Indian state continues to rely on expansive, opaque, and executive-driven frameworks that privilege security imperatives over individual liberties. The persistence of colonial-era rationales within modern legislation, such as the Telecommunications Act, 2023, and the broad exemptions under the Digital Personal Data Protection Act, 2023, brings forward the enduring tension between state sovereignty and citizens' rights in the digital age.

The Pegasus revelations, and subsequent disclosures involving spyware procurement and deployment, have exposed how surveillance practices in India have evolved from tools of exceptional governance into instruments of routine statecraft. Successive governments, irrespective of political affiliation, have consolidated rather than curtailed executive control over data and communications infrastructures. The absence of transparent authorisation procedures, judicial oversight, or independent accountability mechanisms has led to a culture of impunity in which surveillance can be deployed for political or strategic gain under the guise of national security.

Judicial responses, while occasionally affirming privacy in principle, have largely failed to translate constitutional protections into meaningful enforceable safeguards. The Pegasus litigation, marked by sealed cover reports, procedural delays, and judicial deference to executive secrecy, reinforces this institutional oversight. Such failures have not only eroded public trust in constitutional remedies but also risked normalising a condition of perpetual exception, where legality overrides expedience.

In this context, India's digital surveillance regime stands at a critical point. The convergence of outdated colonial statutes, new legislation that replicates and reinforces colonial logic and expansive digital-era laws has created a framework that enables, rather than constraints, state surveillance. Without comprehensive reform, anchored in transparency, proportionality, and independent oversight, India risks institutionalising a surveillance culture incompatible with democratic accountability.

This scoping study interrogates this nexus of law, technology, and power, particularly by tracing how emergent digital laws are reshaping constitutional norms. Only through sustained scrutiny and reform can India reconcile its security goals with the fundamental freedoms at the core of its constitutional democracy.

Works Cited

"Apple warns top Indian opposition leaders, journalists about 'state-sponsored' attack on phone." The Wire, October 31, 2021, https://thewire.in/rights/apple-india-state-sponsored-spyware

"WhatsApp Inc. v. NSO Group Technologies Limited." Global Freedom of Expression. https://globalfreedomofexpression.columbia.edu/cases/whatsapp-inc-v-nso-group-technologies-limited/

Access Now. "Hacking Meduza: Pegasus spyware used to target Putin's critic." Access Now, September 13, 2023, https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/

Access Now. "India's CERT-In must withdraw April directions and strengthen privacy and cybersecurity." Access Now, June 1, 2022, https://www.accessnow.org/press-release/india-cert-in-directions/

Access Now. "NSO to pay $168 million in damages to WhatsApp for Pegasus spyware hacking." Access Now, May 6, 2025, https://www.accessnow.org/press-release/whatsapp-v-nso-case-damages-decision/

Access Now. "Statement on the historic decision in the WhatsApp v NSO case." Access Now, January 13, 2025, https://www.accessnow.org/press-release/statement-on-whatsapp-v-nso-case-decision/

Agamben, Giorgio. State of exception. University of Chicago Press. 2005

Amnesty International. " Global: 'Predator Files' spyware scandal reveals brazen targeting of civil society, politicians and officials." Amnesty International, October 9, 2023, https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/

Amnesty International. "Apple threat notifications: What they mean and what you can do." Amnesty International, April 11, 2024, https://www.amnesty.org/en/latest/news/2024/04/global-apple-threat-notifications-what-they-mean-and-what-you-can-do/

Amnesty International. “Global/India: Apple notifications highlight the unabated threat of unlawful targeted surveillance.” Amnesty International, October 31, 2023, https://www.amnesty.org/en/latest/news/2023/10/global-india-apple-notifications-highlight-the-unabated-threat-of-unlawful-targeted-surveillance/

Amnesty International. “India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists.” Amnesty International, December 28, 2023, https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/

Amnesty International. “India: Human rights defenders targeted by a coordinated spyware operation.” Amnesty International, June 15, 2020, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/

ANI. “Centre purchased Pegasus spyware’ to commit treason, says CM Bhupesh Baghel.” ANI, January 29, 2022, https://www.aninews.in/news/national/general-news/centre-purchased-pegasus-spyware-to-commit-treason-says-cm-bhupesh-baghel20220129181753/

Anurag. “NGO behind Apple’s dubious alert message to politicians is funded by Soros and Ford Foundation.” OpIndia, November 1, 2023, https://www.opindia.com/2023/11/access-now-ngo-behind-warning-messages-sent-on-behalf-of-apple-is-funded-by-soros-and-ford-foundation/

Apple Inc. “About Apple threat notifications and protecting against mercenary spyware.” Apple Support, April 23, 2025, https://support.apple.com/en-in/102174

Arun, P. “In pursuit of personal data: A survey on state surveillance and democracy in India.” In Resilience, fragility, ambivalence, edited by P. R. deSouza, M. S. Alam, and H. Ahmed. Routledge India. 2021. https://doi.org/10.4324/9781003219477

Arun, P. “Penetrative or embracive? Exploring state, surveillance and democracy in India.” In Changing contexts and shifting roles of the Indian state, edited by A. P. D’Costa and A. Chakraborty. Springer. 2019 https://doi.org/10.1007/978-981-13-6891-2_11

Arun, P. “Power to intercept, monitor and surveil: Cybersurveillance and democracy in India.” National Law School Journal, 13, no.1 (2015) https://repository.nls.ac.in/nlsj/vol13/iss1/5

Arun, P. “Uncertainty and Insecurity in Privacyless India: A Despotic Push towards Digitalisation.” Surveillance and Society, 15, no. 3 (2017): 456-464, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/6618/6433/15757

Asher-Schapiro, Avi. “After WhatsApp spyware allegations, Indian journalists demand government transparency.” Committee to Protect Journalists, February 24, 2020, https://cpj.org/2020/02/whatsapp-spyware-allegations-indian-journalists-government/

Ashraf, Merrin Muhammad. (2023, July 6). “Unraveling the digital state of exception in India.” Law School Policy Review. July 6, 2023, https://lawschoolpolicyreview.com/2023/07/06/unraveling-the-digital-state-of-exception-in-india

Bansal, Varsha. “VPN providers flee India as a new data law takes hold.” Wired, September 25, 2022, https://www.wired.com/story/vpn-firms-flee-india-data-collection-law/

Barik, Soumyarendra. “Pegasus: 300 of 1,400 users from India, why ruling may re-open tapping debate.” The Indian Express, December 23, 2024, https://indianexpress.com/article/business/whatsapp-pegasus-ruling-us-india-9737575/

Baxi, Parul. “Technologies of disintermediation in a mediated state: Civil society organisations and India’s Aadhaar project.” South Asia: Journal of South Asian Studies, 42, no. 3 (2019): 554–573. https://doi.org/10.1080/00856401.2019.1602808

Bayly, Christopher Alan. Empire and information: Intelligence gathering and social communication in India, 1780–1870. Cambridge University Press. 2009

Bergman, Ronen, and Mark Mazzetti. (2022, January 28). “The battle for the world’s most powerful cyberweapon.” The New York Times Magazine, January 28, 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

Bhandari, V., & Lahiri, K. (2020). The surveillance state: Privacy and criminal investigation in India—Possible futures in a post-Puttaswamy world. University of Oxford Human Rights Hub Journal, 3(2), 15–36. https://ssrn.com/abstract=3580630

Bhandari, Vrinda, & Renuka Sane. “Protecting citizens from the state post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee report and the Data Protection Bill, 2018.” Socio-Legal Review, 14, no. 2 (2018): 143-169, https://ssrn.com/abstract=3251982

Bhatia, Gautam. “The (continuing) doctrine of judicial evasion in the Aadhaar case.” Constitutional Law and Philosophy, May 9, 2017, https://indconlawphil.wordpress.com/2017/05/09/the-continuing-doctrine-of-judicial-evasion-in-the-aadhaar-case/

Bhatia, Gautam. “The (continuing) doctrine of judicial evasion in the Aadhaar case.” Constitutional Law and Philosophy, May 9, 2017, https://indconlawphil.wordpress.com/2017/05/09/the-continuing-doctrine-of-judicial-evasion-in-the-aadhaar-case/

Bhatia, Gautam. Unsealed covers: A decade of the Constitution, the spurts and the state. Harper Collins, 2023.

Brass, Paul R. “Development of an Institutionalised Riot System in Meerut City, 1961 to 1982.” Economic and Political Weekly, 30, no. 44 (2004): 4839-4848, https://www.jstor.org/stable/4415744

Burman, A. (2023, October 3). Understanding India’s new data protection law. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

Cellan-Jones, Rory. “Coronavirus: Israeli spyware firm pitches to be Covid-19 saviour.” BBC News, April 2, 2020, https://www.bbc.com/news/health-52134452

Centre for Internet and Society. (2015, April 9). “State of Cyber Security and Surveillance in India: A review of the legal landscape.” Centre for Internet and Society, April 9, 2015, https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf

Chandrachud, Chintan. “India - The Kashmir internet restrictions - India’s Supreme Court swaps seats with the executive.” Public Law, no. 4 (2020): 793-795, https://search.informit.org/doi/10.3316/agispt.20200917036801

Chandran, Rina. (2023, March 20). “Surveillance nation: India spies on world’s largest population.” Context News, March 20, 2023, https://www.context.news/surveillance/surveillance-nation-india-spies-on-worlds-largest-population

Chaturvedi, Siddharth, & Himanshi Srivastava. “The constitutionality of the new Indian CERT-In VPN rules.” International Data Privacy Law, 13, no. 4 (2023): 331-337 https://doi.org/10.1093/idpl/ipad015

Chaudhuri, Bidisha. “Distant, opaque and seamful: Seeing the state through the workings of Aadhaar in India.” Information Technology for Development, 27, no. 1 (2020): 37–57. https://doi.org/10.1080/02681102.2020.1789037

Chishti, Seema and Dipankar Ghose. “Surveillance via WhatsApp: On snoop target list—Rights lawyers to activists, DU prof to Defence journalist.” The Indian Express. Novemeber 1, 2019, https://indianexpress.com/article/india/whatsapp-spyware-pegasus-surveillance-india-targets-6097093/

Chishti, Seema. “WhatsApp confirms Israeli spyware was used to snoop on Indian journalists, activists.” The Indian Express, October 31, 2019, https://indianexpress.com/article/india/whatsapp-confirms-israeli-spyware-used-snoop-on-indian-journalists-activists-pegasus-facebook-6095296/

Chishti, Seema. “WhatsApp confirms: Israeli spyware was used to snoop on Indian journalists, activists.” The Indian Express, November 1, 2019 https://indianexpress.com/article/india/whatsapp-confirms-israeli-spyware-used-snoop-on-indian-journalists-activists-pegasus-facebook-6095296/

Choudhury, Deep Kanta Lahiri, and Kenneth A. Loparo. Telegraphic imperialism: Crisis and panic in the Indian empire, c.1830–1920. Palgrave Macmillan. 2010

Choudhury, Deep Kanta Lahiri. “1857” and the communication crisis. Rethinking 1857, edited by S. Bhattacharya. Orient Longman. 2007

Dahat, Pavan., Gopal Sathe, and Aman Sethi. “Bhima Koregaon: Lawyers, activists were among those targeted on WhatsApp by Israeli spyware Pegasus.” HuffPost, October 31, 2019, https://www.huffpost.com/archive/in/entry/whatsapp-hacking-bhima-koregaon-lawyers-targeted_in_5dba8e9ae4b066da552c5028

Deshpande, Swati. “Seven Elgar accused’s phones to be given to Supreme Court Pegasus panel.” The Times of India, February 9, 2022, https://timesofindia.indiatimes.com/city/mumbai/7-elgar-accuseds-phones-to-be-given-to-sc-pegasus-panel/articleshow/89439466.cms

Dharmadhikari, Sanyukta. “The Indian activists, lawyers snooped on through WhatsApp by Israeli spyware Pegasus.” The News Minute, October 31. 2019, https://www.thenewsminute.com/news/indian-activists-lawyers-snooped-through-whatsapp-israeli-spyware-pegasus-111506

ET Online. “Pulwama terror attack: What happened on Feb 14 and how India responded.” The Economic Times, February 14, 2020, https://economictimes.indiatimes.com/news/defence/pulwama-terror-attack-what-happened-on-feb-14-and-how-india-responded/articleshow/74128489.cms

Express News Service. “Pegasus snooping: MHA asks Karnataka government to probe Siddaramaiah’s complaint.” The Indian Express, November 8, 2021, https://indianexpress.com/article/cities/bangalore/pegasus-snooping-mha-asks-karnataka-government-to-probe-siddaramaiahs-complaint-7612364/

Franceschi-Bicchierai, Lorenzo. “Court document reveals locations of WhatsApp victims targeted by NSO spyware.” TechCrunch, April 5, 2024, https://techcrunch.com/2024/04/05/whatsapp-nso-spyware-victims-locations

Ghose, Dipankar. “Chhattisgarh govt sets up panel to probe WhatsApp snoop cloud.” The Indian Express, November 11, 2019, https://indianexpress.com/article/india/chhattisgarh-govt-sets-up-panel-to-probe-whatsapp-snoop-cloud-pegasus-6113600/

Gokhale, Omkar. “Bombay HC seeks state DGIPR’s response on PIL alleging Pegasus link to 2019 Israel study tour.” The Indian Express, August 5, 2021, https://indianexpress.com/article/cities/mumbai/pil-seeks-maharashtra-government-reply-on-2019-study-tour-to-israel-7440147/

Goyal, Prateek. “Bela Bhatia, Anand Teltumbde, Shalini Gera among Indians snooped on using Israeli spyware.” Newslaundry, October 31, 2019, https://www.newslaundry.com/2019/10/31/breaking-bela-bhatia-anand-teltumbde-among-indians-snooped-on-using-israeli-spyware

Gupta, Apar. “Balancing online privacy in India.” Indian Journal of Law and Technology, 6, no. 1 (2010) https://doi.org/10.55496/AULB6542

Gupta, Apar. “Telecom law upgrades for a digital authoritarian state.” The Hindu, December 23, 2023, https://www.thehindu.com/opinion/op-ed/telecom-law-upgrades-for-a-digital-authoritarian-state/article67666811.ece

Gupta, Apar. “Why government’s defence on Apple spyware advisory is weak – and in bad faith.” The Indian Express, November 1, 2023, https://indianexpress.com/article/opinion/columns/apar-gupta-writes-why-governments-defence-on-apple-spyware-advisory-is-weak-and-in-bad-faith-9009581/

HT Correspondent. “Offered to Bengal for ₹25 crore, didn’t buy it: Mamata on Pegasus spying software.” Hindustan Times, March 18, 2022, https://www.hindustantimes.com/india-news/offered-to-bengal-for-rs-25-crore-didn-t-buy-it-mamata-on-pegasus-spying-software-101647544349347.html

HT Correspondent. “Right to privacy not a fundamental right: Centre tells Supreme Court.” Hindustan Times, July 27, 2017, https://www.hindustantimes.com/india-news/right-to-privacy-not-a-fundamental-right-centre-tells-supreme-court/story-bSlTdZjMiAJ0oTEq2gNHPM.html

Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

Jain, Anushka, and Krishnesh Bapat. “In Pegasus battle, the fight for surveillance reform.” The Hindu, December 9, 2022, https://www.thehindu.com/opinion/lead/in-pegasus-battle-the-fight-for-surveillance-reform/article65667538.ece

Jain, Debby. “Nothing wrong in country using spyware for security; Question is against whom it's used: Supreme Court in Pegasus case.” Live Law, April 29, 2025, https://www.livelaw.in/top-stories/supreme-court-pegasus-spyware-judicial-probe-into-illegal-surveillance-290684

K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2018) 1 SCC 809.

K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1 (India).

Kant J, Surya, and N.K. Singh J. “Manohar Lal Sharma v. Prime Minister: Pegasus spyware probe case – Background.” Supreme Court Observer, July 16, 2025, https://www.scobserver.in/cases/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-case-background/

Madhyamam Broadcasting Limited v. Union of India, 2023 SCC OnLine SC 366.

Mahaprashasta, Ajoy Ashirwad. “Days After Accusing CJI Gogoi of Sexual Harassment, Staffer Put on List of Potential Snoop Targets,” The Wire, Junly 19, 2021, https://thewire.in/rights/ranjan-gogoi-sexual-harassment-pegasus-spyware

Mahaprashasta, Ajoy Ashirwad. (2021, July 20). “Leaked snoop list suggests surveillance may have played role in toppling of Karnataka govt in 2019.” The Wire, July 20, 2021, https://m.thewire.in/article/politics/karnataka-government-toppling-pegasus-spyware-surveillance

Malhotra, Gayatri. “Delhi HC issues notice on writ petition seeking extent of e-surveillance carried out by MHA under S 69 of IT Act.” Internet Freedom Foundation, March 22, 2023, https://internetfreedom.in/delhi-hc-issues-notice-on-writ-petition-seeking-extent-of-e-surveillance-carried-out-by-mha-under-s-69-of-it-act/

Malhotra, Gayatri. “India’s new data protection law: No transparency, no privacy.” Context News, August 17, 2023, https://www.context.news/surveillance/opinion/indias-new-data-protection-law-no-transparency-no-privacy

Manohar Lal Sharma (Pegasus Spyware) v. Union of India, (2023) 11 SCC 401, decided on October 27, 2021.

Marczak, Bill., John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. (2018, September 18). “Hide and seek: Tracking NSO Group’s Pegasus spyware to operations in 45 countries.” The Citizen Lab, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Ministry of Communications. “The Telecommunications Act 2023: Ushering in a new era of connectivity.” Press Information Bureau, July 5, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2031057

Ministry of Electronics and IT. “CERT-In issues directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet.” Press Information Bureau, April 28, 2022, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1820904

Mukhopadhyay, Devdutta. “Statement: IFF joins international civil society orgs to oppose the NSO Group’s attempt to evade responsibility for the Pegasus hack #SaveOurPrivacy.” Internet Freedom Foundation, December 24, 2020, https://internetfreedom.in/ninth-circuit-amici-brief-whatsapp-nso-group-pegasus-hack/

Ojha, Shristi. “BREAKING: Supreme Court stays probe of Justice Lokur Commission constituted by WB Govt in Pegasus case.” Live Law, December 17, 2021 https://www.livelaw.in/top-stories/supreme-court-restrains-justice-lokur-commission-constituted-by-wb-govt-from-probing-pegasus-case-187885

Panjiar, Tejasi, & Malhotra, Gayatri. “A draft to surveil: IFF’s analysis of the Draft Telecom Interception Rules, 2024.” Internet Freedom Foundation, September 12, 2024, https://internetfreedom.in/telecom-interception-rules-2024-analysis/

Parashar, Utpal. “‘International conspiracy to defame India’: Assam CM on Pegasus row.” Hindustan Times, July 20, 2021, https://www.hindustantimes.com/india-news/international-conspiracy-to-defame-india-assam-cm-on-pegasus-row-101626796355634.html

Pathak, Subhash. “Pegasus row: Bihar CM seeks detailed probe into allegations of phone-hacking.” Hindustan Times, August 2, 2021, https://www.hindustantimes.com/cities/patna-news/pegasus-row-bihar-cm-seeks-detailed-probe-into-allegations-of-phone-hacking-101627911806760.html

Press Trust of India. “Centre taps over 1 lakh phones a year; Many more by states.” *Business Standard*, September 4, 2014, https://www.business-standard.com/article/pti-stories/centre-taps-over-1-lakh-phones-a-yr-many-more-by-states-114090400673_1.html

PTI. “Govt to probe Oppn MPs’ claims of getting hacking attempt warnings from Apple.” Deccan Herald, October 31, 2023, https://www.deccanherald.com/india/govt-orders-probe-after-opposition-mps-claims-of-receiving-hacking-attempt-warnings-from-apple-2749839/

PUCL v. Union of India, (1997) 1 SCC 301.

Rajagopal, Krishnadas. “Supreme Court asks what’s wrong if country using Pegasus against ‘anti-nationals,’ agrees to examine if private citizens were hacked.” The Hindu, April 29, 2025, https://www.thehindu.com/news/national/pegasus-row-supreme-court-says-wont-disclose-report-that-touches-countrys-security-sovereignty/article69504285.ece

Rao, Hitender. “Pegasus spyware: Khattar questions Amnesty International’s credibility.” Hindustan Times, July 22, 2021, https://www.hindustantimes.com/cities/chandigarh-news/pegasus-spyware-khattar-questions-amnesty-international-s-credibility-101626893867660.html

Rath, Saroj Kumar. “New terror architecture in South Asia: 26/11 Mumbai attacks inquiry.” India Quarterly, 66, no. 4 (2011): 359–378. https://doi.org/10.1177/097492841006600403

Reynolds, John. Empire, emergency and international law. Cambridge University Press. 2017

Rupesh Kumar & Others v. Union of India & Others, Redacted Writ Petition, Supreme Court of India, July 31, 2021. https://drive.google.com/file/d/1dgXAOtvBrXc6YFUDfB4THu4AKix1RvYE/view

Sachdev, Vakasha. “5 Pegasus victims move SC, decry 'state-sponsored illegal hacking'.” The Quint, August 2, 2021, https://www.thequint.com/news/law/paranjoy-guha-thakurta-snm-abdi-prem-shankar-jha-rupesh-kumar-singh-ipsa-shatakshi-say-use-of-spyware-against-them-was-illegal-hacking-not-lawful-surveillance

Samdani, M. N. “Andhra Pradesh: TDP govt didn’t buy Pegasus spyware, says N. Chandrababu Naidu.” Times of India, March 19, 2022, https://timesofindia.indiatimes.com/city/amaravati/andhra-pradesh-tdp-govt-didnt-buy-pegasus-spyware-says-n-chandrababu-naidu/articleshow/90314865.cms

Sanjeev Sanyal “Very curious indeed. The security threat messages being received by some prominent Apple users is not quite from Apple but from a Soros-linked NGO called http://accessnow.org. How is this external agency able to send such authentic looking messages though the system??” X, November 1, 2023. https://x.com/sanjeevsanyal/status/1719571401546297629

Scroll Staff. “Pegasus: Centre refuses to file affidavit in SC on surveillance allegations, cites national security.” Scroll, September 13, 2021, https://scroll.in/latest/1005257/pegasus-centre-refuses-to-file-affidavit-in-sc-on-surveillance-allegations-cites-national-security

SFLC. “Comments on the Draft Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024.” Software Freedom Law Centre, October 10, 2024, https://sflc.in/comments-on-the-draft-telecommunications-procedures-and-safeguards-for-lawful-interception-of-messages-rules-2024/

Sharma, Nalini. “A peek into ML Sharma’s world of publicity interest litigation.” India Today, July 23, 2021, https://www.indiatoday.in/law/story/peek-manohar-lal-sharma-world-public-interest-litigation-1831753-2021-07-23

Singh, P. Sujatha. (2022, March 18). “Pegasus had offered its spyware, but TDP government rejected it, says Lokesh.” The Hindu, March 18, 2022, https://www.thehindu.com/news/national/andhra-pradesh/pegasus-had-offered-its-spyware-but-tdp-government-rejected-it-says-lokesh/article65234861.ece

Singh, P. Sujatha. (2022, March 18). “Pegasus had offered its spyware, but TDP government rejected it, says Lokesh.” The Hindu, March 18, 2022, https://www.thehindu.com/news/national/andhra-pradesh/pegasus-had-offered-its-spyware-but-tdp-government-rejected-it-says-lokesh/article65234861.ece

Singh, Shiv Sahay. “Pegasus spyware issue: West Bengal govt. sets up two-member inquiry commission.” The Hindu, July 27, 2021, https://www.thehindu.com/news/cities/kolkata/pegasus-spyware-issue-west-bengal-govt-sets-up-two-member-inquiry-commission/article35534671.ece

Singh, Tanmay. “India’s new intermediary guidelines: The gloves come off in the assault on civil liberties.” Verfassungsblog: On Matters Constitutional, June 1, 2021, https://doi.org/10.17176/20210602-003803-0

Singh, Vijaita. “Central government exempts CERT-In from RTI Act.” The Hindu, November 25, 2023, https://www.thehindu.com/news/national/central-government-exempts-cert-in-from-rti-act/article67569804.ece

Special Correspondent. “New online platform maps Pegasus spread.” The Hindu, July 7, 2021, https://www.thehindu.com/news/national/new-online-platform-maps-pegasus-spread/article35185350.ece

Srivas, Anuj., and Kabir Agarwal. “Snoop list has 40 Indian journalists, forensic tests confirm presence of Pegasus spyware on some.” The Wire, July 18, 2021, https://thewire.in/media/pegasus-project-spyware-indian-journalists/

Srivastava, Mehul., and Kaye Wiggins. “India hunts for spyware that rivals controversial Pegasus system.” Financial Times, March 30, 2023, https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9

Supreme Court Observer. “Pegasus spyware probe #6: Court refuses to stay activities of West Bengal commission.” Supreme Court Observer, December 17, 2021, https://www.scobserver.in/reports/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-day-6-oral-hearings/

Thumfart, Johannes. “Digital rights and the state of exception: Internet shutdowns from the perspective of just securitization theory.” Journal of Global Security Studies, 9, no.1 (2024) https://doi.org/10.1093/jogss/ogad024

TNN. “Bengal was offered Pegasus for Rs 25 crore 4–5 years ago, says Mamata Banerjee.” Times of India, March 18, 2022, https://timesofindia.indiatimes.com/city/kolkata/mamata-pegasus-was-on-offer-for-25-crore/articleshow/90300716.cms

Union of India. (2021, August 16). Limited affidavit on behalf of Union of India. https://drive.google.com/file/d/1U1BluslRyS1Qk3awdFf9QUyM1hGeg-gq/view

Varadarajan, Siddharth. “Pegasus Project: How phones of journalists, ministers, activists may have been used to spy on them.” The Wire, July 18, 2021, https://thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying/

Varma, P. Sujatha. “Pegasus had offered its spyware, but TDP government rejected it, says Lokesh.” The Hindu, March 18, 2022, https://www.thehindu.com/news/national/andhra-pradesh/pegasus-had-offered-its-spyware-but-tdp-government-rejected-it-says-lokesh/article65234861.ece

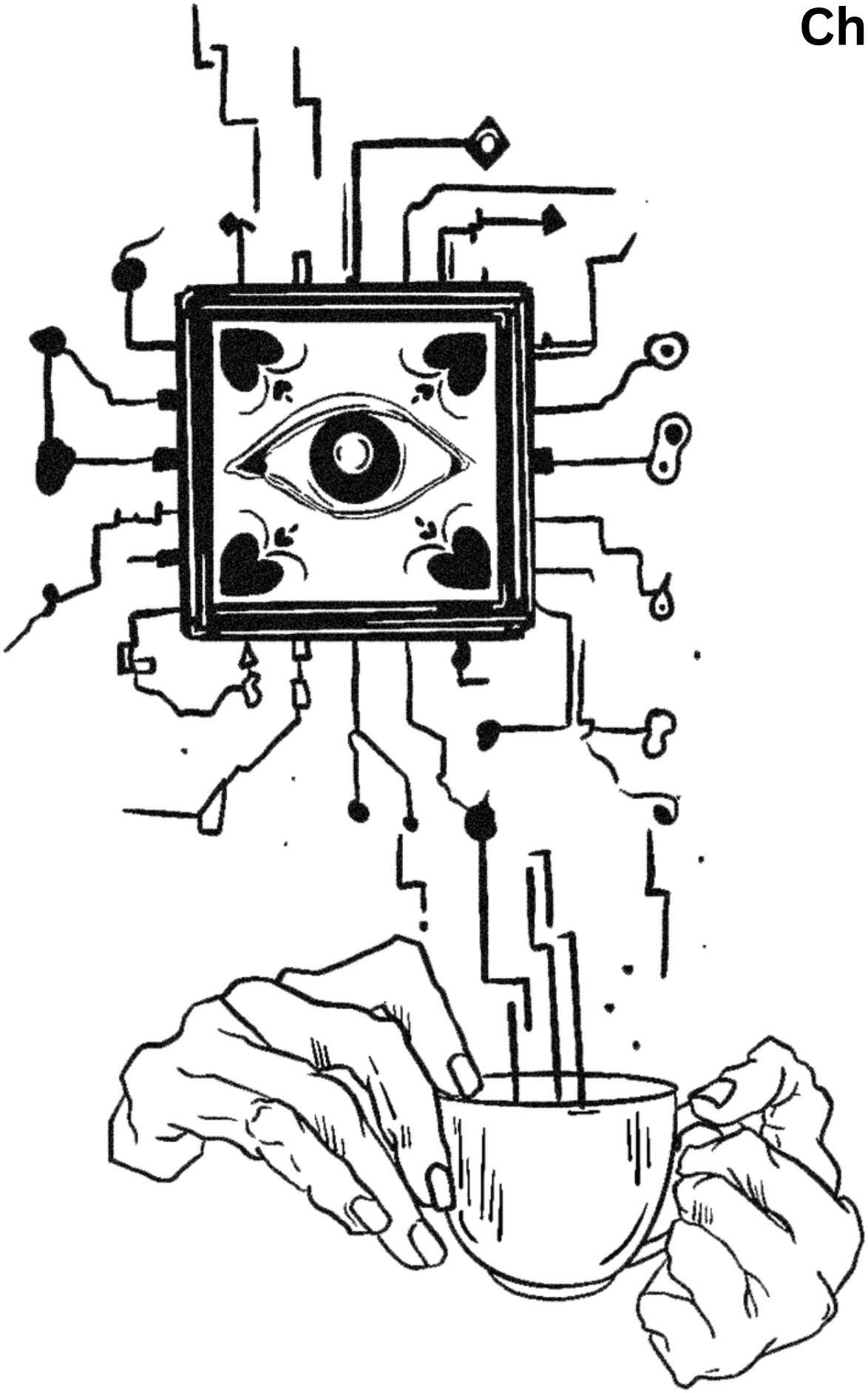
Vijayaraghavan, Venkatesh, and Sameer Singh. “‘Look But Don’t Touch: A Critique of the Indian Position on Evidence Illegally Obtained Through Tape Recordings." National Law School of India Review, 12, no. 1, (2000) https://repository.nls.ac.in/nlsir/vol12/iss1/8/

Washington Post. “Takeaways from the Pegasus Project.” The Washington Post, February 2, 2022, https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/

Xavier, John. “WhatsApp vs Government | Why exiting India threat bestirs 'traceability' debate.” The Hindu, April 27, 2024, https://www.thehindu.com/sci-tech/technology/whatsapp-vs-government-why-exiting-india-threat-bestirs-traceability-debate/article68113037.ece

SRI LANKA

Chapter 4



DRF USA

Abbreviations

BIA	Bandaranaike International Airport
CDRD	Centre for Defence Research and Development
CERT	Computer Emergency Response Team
CPA	Centre for Policy Alternatives
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessments
IPKF	Indian Peace Keeping Force
ISP	Internet Service Providers
LTTE	Liberation Tigers of Tamil Eelam
MOSIP	Modular Open-Source Identity Platform
MOU	Memoranda of Understanding
NIC	Digital National Identity Card

PDPA	Personal Data Protection Act
RCS	Remote Control System
SIS	State Intelligence Service
SOP	Standard Operating Procedures

Introduction

The evolution of surveillance in Sri Lanka mirrors the country's broader political trajectory, shaped by protracted civil conflict, authoritarian governance, and the recurring invocation of national security to justify exceptional state powers. For decades, the rhetoric of security and stability has enabled successive governments to normalize intrusive surveillance practices, from traditional intelligence monitoring during the civil war to modern cyber espionage in the digital age. These developments have taken place in an environment of limited public scrutiny and weak legal oversight, where privacy and civil liberties are routinely subordinated to state interests.

Sri Lanka's surveillance apparatus has not emerged in isolation. It is the product of intersecting historical, technological, and geopolitical forces. The country's early exposure to military surveillance during the civil war years (1983 - 2009) laid the groundwork for a permanent culture of monitoring, particularly in the North and East. Post-war, this infrastructure evolved into a complex digital ecosystem driven by global spyware procurement, foreign partnerships, and a growing appetite for domestic cyber capabilities. As digitalization accelerates, so too has the state's capacity to intrude into private communications, track dissent, and control information flows. This convergence of security, technology, and politics underscores a crucial question – how can a state balance its legitimate security concerns with the protection of fundamental rights in the digital era?

While this chapter focuses on Sri Lanka's surveillance landscape through an analysis of documented evidence and expert testimony, it is important to underscore from the get go a glaring limitation and imbalance inherent to this report – a lack of evidentiary information in the public domain makes it difficult to say anything with certainty. It is impossible to know exactly how or to what extent surveillance technologies have been acquired and/or deployed by Sri Lankan authorities but this report tries its best to piece together what is known.

Historical Context

In Sri Lanka, “national security” has consistently been used to justify arbitrary state action, such as surveillance and cyber intrusion which violate the rights of citizens. The lack of public awareness around how such intrusions impede on privacy has allowed the state to monitor civilians, journalists, ethnic minorities, human rights defenders and political opponents. Successive governments have facilitated purchases of nearly 40 million USD worth of surveillance technology with minimal public outcry. As a result, whether during times of civil conflict, political transition, or post-war governance, national security has provided the necessary cover to expand and normalize surveillance practices, often with limited transparency and virtually no accountability.[1]

Sri Lanka’s repressive political trajectory is aided by a long-standing culture of surveillance. During the civil war (1983–2009), the state’s security apparatus expanded significantly, especially in the North and East - homeland of the minority Tamil community, where an extensive intelligence and military presence remains to this day. Originally justified by the need to combat the Liberation Tigers of Tamil Eelam (LTTE), a separatist militant organization later proscribed as a terrorist group in many countries, this infrastructure has enabled prolonged militarization and surveillance in these regions.[2]

In particular, the deployment of the Indian Peace Keeping Force (IPKF) as part of the Indo-Sri Lanka Accord in 1987 introduced advanced military surveillance technology into Sri Lanka’s existing security framework. While the IPKF was intended to act as a neutral peacekeeping force, its presence paved the way for increased intelligence capabilities, which successive Sri Lankan governments continued to exploit post-conflict.

[1] Charya Samarkoon & Bhavani Foneska, ‘Right to Privacy in Sri Lanka,’ Center for Policy Alternatives, September 2020, https://www.cpalanka.org/wp-content/uploads/2020/09/Discussion-Paper-Right-to-Privacy-updated-draft-4-1.pdf (accessed on 1 September 2025)

[2] Human Rights Watch, ‘Sri Lanka: Reject New Counterterrorism Bill,’ Human Rights Watch, 7 April 2023, https://www.hrw.org/news/2023/04/07/sri-lanka-reject-new-counterterrorism-bill (accessed on 1 September 2025)

Following the LTTE's defeat in 2009, surveillance intensified as state actors used telecommunication towers to monitor mobile phone signals to track, threaten, and abduct journalists who were critical of the government. Cyber intrusions became especially widespread during President Mahinda Rajapaksa's administration (2005–2015), as phone tapping was used to target any dissenting voice in Sri Lanka's socio-political sphere. In 2009 for example, Lasantha Wickrematunge, editor of the investigative paper The Sunday Leader, was killed in a state-commissioned attack following which a leaked intelligence report labelled him a "national security risk." The report further admitted that his phone was being tapped weeks before his assassination, allegedly by a paramilitary group linked to then Defence Secretary Gotabaya Rajapaksa.[3]

In 2014, efforts to modernize Sri Lanka's surveillance infrastructure included attempts by the National Intelligence Bureau (NIB) (now referred to as the State Intelligence Service (SIS)) to procure Remote Control System (RCS) spyware, acquired from Italy-based company Hacking Team.[4] These leaks were found alongside allegations made by local brokers towards other law enforcement agencies such as the Sri Lankan Police and its Criminal Investigation Department (CID), said to be potential buyers of the technology. Relatedly, telecommunication companies faced routine government requests for user data – a practice confirmed both by telecom operators themselves and new outlets. Chief Executive of leading telecom Dialog Axiata, Dr. Hans Wijesuriya stated that telecom operators were required to comply with such government requests.[5]

[3] Tamil Guardian, 'Sri Lankan defence secretary tapped murdered journalist's phone,' Tamil Guardian, 4 November 2016, https://www.tamilguardian.com/content/sri-lankan-defence-secretary-tapped-murdered-journalists-phone (accessed on 1 September 2025)

[4] WikiLeaks, Hacking Team email archives related to Sri Lanka, WikiLeaks, 8 July 2015, https://wikileaks.org/hackingteam/emails/emailid/593346 (accessed on 1 September 2025)

[5] Freedom House, 'Freedom on the Net 2014: Sri Lanka,' Freedom House, 4 December 2014, https://www.refworld.org/reference/annualreport/freehou/2014/en/102727 (accessed on 1 September 2025)

This was also a time when surveillance extended to political opposition figures, forcing them to use burner phones and coded language. In fact, the Rajapaksa regime monitored its own party ranks. In 2014, as general secretary Maithripala Sirisena and cabinet ministers began to defect, they swapped out their phones for trusted devices to avoid government wiretaps.[6] Even former President Chandrika Bandaranaike Kumaratunga admitted to using encrypted platforms like Viber - an instant messaging application that, at the time, was believed to be difficult to tap into by Sri Lankan intelligence agencies.[7] Similarly, following Sri Lanka's general elections of 2015, news reports confirmed that the SIS was monitoring telephone records of "politicians, media personnel, former ministers, diplomats and police officers," under the direction of the Ministry of Defence.[8]

The election of the 'Good Governance' coalition in 2015 brought hopes for reform particularly to the surveillance conditions in the country and while the passing of the Right to Information Act (2016) was a step forward, exemptions made on matters of national security ensured surveillance activities remained beyond public scrutiny.[9] The Easter Sunday attacks in 2019, which killed over 250 people, marked a pivotal shift in surveillance policy. According to an investigation conducted by a Sri Lankan parliamentary committee, it was found that the bombers had used encrypted apps like Threema, prompting Sri Lankan authorities to further expand their surveillance apparatus.[10] With assistance from India, the United States, and Turkey, aggressive cyber investigations were conducted to access digital footprints and private communications of suspected bombers and their network. While these efforts were framed as necessary to prevent future terror attacks, concerns remain about the continued use of these surveillance tools and the threat of privacy violations.[11]

---

[6] Sanjana Hattotuwa, 'Hacking the hackers: Surveillance in Sri Lanka revealed,' GroundViews, 15 July 2015, https://groundviews.org/2015/07/15/hacking-the-hackers-surveillance-in-sri-lanka-revealed/ (accessed on 1 September 2025)

[7] Ada Derana, 'CBK reveals why she used Viber to topple MR,' Ada Derana, 6 September 2015, https://www.adaderana.lk/news.php?nid=32243 (accessed on 1 September 2025)

[8] Sri Lankan Guardian, 'Intelligence Chief Quits; Telephone Tapping Stops," Sri Lanka Guardian, 18 January 2015, https://web.archive.org/web/20240327012547/http://www.srilankaguardian.org/2015/01/intelligence-chief-quits-telephone.html (accessed on 1 September 2025)

[9] Charya Samarkoon & Bhavani Foneska, 'Right to Privacy in Sri Lanka,' Center for Policy Alternatives, September 2020, https://www.cpalanka.org/wp-content/uploads/2020/09/Discussion-Paper-Right-to-Privacy-updated-draft-4-1.pdf (accessed on 1 September 2025)

[10] Hon. J.M. Ananda Kumarasiri, 'Report of the Select Committee of Parliament to look into and report to Parliament on the Terrorist Attacks that took place in different places in Sri Lanka on 21st April 2019,' Parliament of Sri Lanka, 23 October 2019, https://www.parliament.lk/uploads/comreports/sc-april-attacks-report-en.pdf (accessed on 1 September 2025)

[11] Freedom House, 'Freedom on the Net 2020: Sri Lanka,' Freedom House, 2020, https://freedomhouse.org/country/sri-lanka/freedom-net/2020 (accessed on 1 September 2025)

Moreover, prior to the bombings, former President Maithripala Sirisena had already sought Cabinet approval for a purchase of up to 38.9 million USD in surveillance technology from an unnamed Israeli company, effectively bypassing procurement rules.[12] This compromised paper trail - reported on and published by the Colombo Telegraph - clearly shows evidence of the government's procurement plans for intrusive capabilities alongside confirmation of the fact that such tools were not being used to ensure national security. He also requested Chinese support to acquire tools capable of monitoring encrypted platforms, ostensibly to aid his anti-drug campaign.[13]

The return of the Rajapaksas to power in late 2019 brought with it a renewed state surveillance. President Gotabaya Rajapaksa and Prime Minister Mahinda Rajapaksa both capitalized on post-Easter attack fears and rising anti-Muslim sentiments by arguing that monitoring digital communications was essential to combating terrorism and cybercrime. In 2021, the Cabinet approved plans for two key bills: the “Defence Cyber Commands” Bill and a general “Cybersecurity Bill”. These billsaimed to empower cyber units within the country’s law enforcement institutions with the power to act on national security matters and proposed the establishment of the Sri Lanka Cyber Protection Agency respectively.

The return of the Rajapaksas to power in late 2019 brought with it a renewed state surveillance. President Gotabaya Rajapaksa and Prime Minister Mahinda Rajapaksa both capitalized on post-Easter attack fears and rising anti-Muslim sentiments by arguing that monitoring digital communications was essential to combating terrorism and cybercrime. In 2021, the Cabinet approved plans for two key bills: the “Defence Cyber Commands” Bill and a general “Cybersecurity Bill”. These billsaimed to empower cyber units within the country’s law enforcement institutions with the power to act on national security matters and proposed the establishment of the Sri Lanka Cyber Protection Agency respectively.

[12] Colombo Telegraph, ‘Sri Lankan Govt to Spend 6.9 Billion Rupees for Interception Equipment,’ Colombo Telegraph, 21 March 2019, https://www.colombotelegraph.com/index.php/sri-lankan-govt-to-spend-6-9-billion-rupees-for-interception-equipment/ (accessed on 1 September 2025)

[13] Freedom House, ‘Freedom on the Net 2020: Sri Lanka,’ Freedom House, 2020, https://freedomhouse.org/country/sri-lanka/freedom-net/2020 (accessed on 1 September 2025)

Simultaneously, opposition politicians have accused the government of using Pegasus to monitor critics. Though these claims were denied, officials had admitted that intelligence services were using different methods for the security of the country.[14] Vaguestatements such as this along with the absence of transparency and oversight continues to fuel speculation and mistrust amidst the Sri Lankan public.

With the 2022 economic crisis and the Aragalaya (uprising) protests, activists and protest leaders reported increased monitoring by security forces, particularly through social media. One high-profile case involved a youth activist being arrested for creating a Facebook group critical of President Gotabaya Rajapaksa (The Sunday Times, 2022)[15]. During protests, people encouraged ethical cyber intrusion, inviting groups like Anonymous to target government systems. A large social media movement emerged in April 2022, with the hashtag #AnonymousSaveSriLanka, urging cyberattacks on government websites to expose corruption within government ranks. However, cybersecurity experts raised concerns about such actions, warning that hacking government sites could lead to the public exposure of sensitive information.

Following Gotabaya Rajapaksa's resignation, President Ranil Wickremesinghe's interim government continued using surveillance and legal measures to suppress dissent. His administration introduced several controversial bills, including the Online Safety Bill and the Rehabilitation Bill, both containing provisions that added surveillance measures to existing legislation.

On the onset of 2025, Sri Lanka saw a new government take office, one that pledged to repeal and/or amend draconian laws (including surveillance measures) passed under previous administrations. However, balancing domestic reform with geopolitical pressures has proven challenging. Recent proposals for a Digital National Identity Card (NIC), backed by the Indian government and modeled after Aadhaar, has sparked widespread concerns on foreign access to sensitive information and state surveillance under the guise of digital modernization.

---

[14] Maheesha Mudugamuwa, 'Controversial Pegasus spyware: Govt dismisses using the spyware,' The Morning, 24 July 2021, https://www.themorning.lk/controversial-pegasus-spyware-govt-dismisses-using-the-spyware/ (accessed on 1 September 2025)

[15] The Sunday Times, 'Youth activist behind #GoHomeGota Facebook campaign arrested and produced in Court,' The Sunday Times, 3 April 2022, https://www.sundaytimes.lk/220403/news/youth-activist-behind-gohomegota-facebook-campaign-arrested-and-produced-in-court-479036.html (accessed on 1 September 2025)

Despite the misuse of cyber intrusive capabilities, public awareness regarding data privacy and its implications for citizens remains low. Sri Lanka's cybersecurity infrastructure remains underdeveloped and initiatives to build cybersecurity capacity have been inconsistent, especially when compared to investments in spyware technologies. The following chapter will detail the surveillance landscape for both covert and overt cyber intrusions, their potential targets, and risks for privacy and digital rights.

Findings on Surveillance in Sri Lanka

The Evolving Landscape of State Surveillance

Sri Lanka's government has a historical precedent of seeking sophisticated cyber intrusion and surveillance capabilities, a trend that has prompted significant debates about the balance between national security, privacy, and fundamental human rights. The country's history of civil conflict and political unrest has shaped a security apparatus that remains deeply concerned with monitoring threats, whether real or perceived, in the name of maintaining peace and stability. In this context, this section presents a narrative analysis of how Sri Lanka has pursued and utilized cyber intrusion tools.

We begin by first setting the historical context for state surveillance in the country and then move onto Sri Lankan authorities' concerted efforts to obtain modern digital surveillance technology, focusing on the procurement of commercial spyware and the development of domestic capabilities. This section also explores the critical impact of foreign influences on state surveillance, particularly from China, Israel, and India, and the geopolitical dimensions of these partnerships. Finally, it assesses public perceptions of the state's surveillance powers and the resulting climate of fear and mistrust. The analysis presented below draws heavily on documented evidence, official reports, and expert interviews with professionals in media, cybersecurity, and technology law.

History of State Surveillance in Sri Lanka

Sri Lanka's history of civil war has had a notable impact on the architecture and culture of state surveillance. As detailed previously, evidence has emerged that during the civil war (1983–2009) and its immediate aftermath, government intelligence agencies closely monitored communications, albeit with limited digital capabilities at the time. This surveillance was particularly targeted towards journalists reporting on wartime impunity and human rights violations, as well as those perceived as sympathetic to the Liberation Tigers of Tamil Eelam (LTTE).[16]

[16] Heshan Maduranga, 'Cybercrime Analysis – Sri Lanka,' Cardiff Metropolitan University, 4 May 2023, https://www.researchgate.net/publication/378336517_Cybercrime_Analysis_-_Sri_Lanka (accessed on 1 September 2025)

According to Mandana Ismail, a veteran journalist the term “cyber surveillance” was not in common use during the 1990s and early 2000s, yet journalists at the time operated under a presumption of constant watch. This was due to the widespread use of traditional surveillance methods, including phone tapping, physical interception of communications, the bugging of offices and homes, and informal censorship. This environment fostered a "climate of fear" that persists to this day, particularly in the North-East, where a heavy military and intelligence presence continues to monitor and intimidate the Tamil community, civil society organizations, and media personnel.[17]

As described by Mandana, journalists developed creative countermeasures to evade government surveillance, such as sharing common e-mail accounts where messages were saved as drafts instead of being sent, using public phones, or employing temporary e-mail addresses for sensitive communications. These tactics indicate an early and acute awareness of state monitoring, a historical precedent that continues to shape contemporary anxieties regarding privacy in Sri Lanka.

Efforts to Gain Access to Modern Digital Surveillance Technology

In the post-war era, Sri Lankan authorities began a concerted effort to modernize their surveillance toolkit, moving from traditional methods to more sophisticated cyber intrusion capabilities. This transition has been characterized by two primary approaches: the pursuit of commercial spyware from the global market and the development of indigenous surveillance technologies.

[17] Adayaalam Centre for Policy Research, ‘A phantom that is Real: Persisting Culture of Surveillance and Intimidation in the North-East, Adayaalam Centre for Policy Research, February 2025, https://adayaalam.org/wp-content/uploads/2025/05/A-Phantom-that-is-Real_-Persisting-Culture-or-Surveilance-and-Intimidation-in-the-NorthEast.pdf (accessed on 1 September 2025)

Evidence of Spyware Procurement and Interest

Leaked documents and public allegations reveal a consistent state appetite for advanced offensive cyber tools, often procured with minimal transparency.

Hacking Team: In 2013, leaked documents first published by WikiLeaks in 2015 exposed that Sri Lanka's intelligence officials had approached the Italian company Hacking Team, an infamous vendor of offensive intrusion software.[18] Internal emails from the company confirmed that private actors in Sri Lanka had requested information about its flagship service (possibly for brokered sales to the state), Remote Control System (RCS) spyware. While the meetings were described as having a "positive" outcome, the procurement was reportedly unsuccessful due to budget limitations. This dialogue continued into 2014, with Hacking Team being informed that Sri Lanka's Ministry of Defence intended to develop its own "electronic surveillance and tracking system" in collaboration with a local university. Despite this, representatives of the Sri Lanka Police and Criminal Investigation Department were still negotiating for a live demonstration of Hacking Team's tools later that year, underscoring the state's active pursuit of cutting-edge spyware.

Pegasus: More recently, global revelations surrounding the highly intrusive Pegasus spyware, developed by the Israeli NSO Group, have fueled concerns in Sri Lanka. Pegasus is a formidable "zero-click" spyware, meaning it can infect a device without any interaction from the user, granting the attacker complete and unrestricted access to all data and sensors on the device, including the camera, microphone, and GPS.[19] In 2021, opposition Member of Parliament Harin Fernando accused the government of using Pegasus against political opponents and activists. While the government denied the accusation, Cabinet Minister Keheliya Rambukwella acknowledged that intelligence agencies might employ "other methods" for national security purposes, a statement that did little to quell public mistrust.[20] The global Pegasus Project investigation revealed that the spyware was used worldwide to target journalists, human rights defenders, and political figures, making the allegations in Sri Lanka highly plausible within the regional context of shrinking civic space.[21]

---

[18] Alex Hern, 'Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim,' The Guardian, 6 July 2015, https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim (accessed on 1 September 2025)

[19] Tamar Kaldani, & Zeev Prokopets, 'Pegasus Spyware Report and its impact on human rights,' Council of Europe, April 2022, https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8 (accessed on 1 September 2025)

[20] The Sunday Times, 'Youth activist behind #GoHomeGota Facebook campaign arrested and produced in Court,' The Sunday Times, 3 April 2022, https://www.sundaytimes.lk/220403/news/youth-activist-behind-gohomegota-facebook-campaign-arrested-and-produced-in-court-479036.html (accessed on 1 September 2025)

[21] Forbidden Stories, 'The Pegasus Project: Global democracy under cyber attack,' Forbidden Stories, 18 July 2021, https://forbiddenstories.org/about-the-pegasus-project/ (accessed on 1 September 2025)

FinFisher: Similar uncertainties exist regarding FinFisher, another commercial spyware suite marketed to governments. Suspicions about its use in Sri Lanka have grown due to its documented deployment in other repressive regimes and recurring patterns of digital surveillance locally. While a 2015 report by WikiLeaks listed Sri Lanka among countries where FinFisher command-and-control servers were detected, a detailed investigation by Citizen Lab in the same year, which mapped FinFisher's global proliferation, did not include Sri Lanka in its list of 32 likely government users.[22] This discrepancy highlights the difficulty in definitively confirming the use of such tools in an environment of state secrecy, though it does not eliminate the possibility of its deployment.

2019 Israeli Firm Procurement: A notable instance of secretive procurement occurred in 2019 when then-President Maithripala Sirisena, in his capacity as Defence Minister, proposed a classified cabinet memorandum to urgently purchase advanced surveillance equipment from an undisclosed Israeli firm for USD 38.9 million.[23] The memorandum, justified as necessary to combat drug trafficking, explicitly sought to bypass standard, transparent procurement processes, citing the need for "secrecy and confidentiality" and withholding critical details from the Cabinet itself.[24] This move underscored the government's intent to acquire sophisticated interception capabilities from the global spyware market, a trend that continues to raise alarms among digital rights advocates.[25]

---

[22] Bill Marczak, John Scott-Railton, Adam Senft, Irene Petranto, & Sarah McKune, 'Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation,' Citizen Lab, 15 October 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ (accessed on 1 September 2025)

[23] Colombo Telegraph, 'Sri Lankan Govt to Spend 6.9 Billion Rupees for Interception Equipment,' Colombo Telegraph, 21 March 2019, https://www.colombotelegraph.com/index.php/sri-lankan-govt-to-spend-6-9-billion-rupees-for-interception-equipment/ (accessed on 1 September 2025)

Freedom House, 'Freedom on the Net 2019: Sri Lanka,' Freedom House, 2019, https://freedomhouse.org/country/sri-lanka/freedom-net/2019 (accessed on 1 September 2025)

[24] Ibid

[25] Ibid

Domestic Surveillance Development

Parallel to its efforts to procure foreign technology, the Sri Lankan state has pursued a long-term strategy of building indigenous surveillance capacity. This approach aims to reduce reliance on foreign vendors, who may be subject to international pressure or export controls, and create a more resilient, self-sufficient state surveillance apparatus.

This "build" strategy is spearheaded by the Centre for Defence Research and Development (CDRD), a research and development institute operating under the Ministry of Defence. The CDRD's mandate includes the development of technology for the armed forces, and contains a dedicated "Surveillance Wing" responsible for R&D in tactical and strategic surveillance, reconnaissance, and remote sensing.[26]

The CDRD actively collaborates with local universities to leverage academic expertise. It has signed Memoranda of Understanding (MOUs) and engaged in joint projects with a network of institutions, including the University of Moratuwa, University of Peradeniya, University of Ruhuna, University of Sri Jayewardenepura, and NSBM Green University. This systemic collaboration to develop domestic surveillance and tracking systems validates the information noted in the 2014 Hacking Team emails, where the Ministry of Defence expressed its intent to develop a local "electronic surveillance and tracking system" with a university partner. These projects include the development of unmanned aerial vehicles (UAVs), geospatial monitoring platforms, and maritime surveillance systems using machine learning.[27]

---

[26] Centre for Defence Research & Development, https://crd.lk/ (accessed on 1 September 2025)

[27] Ministry of Defence, 'Defence Research and Development Projects,' Ministry of Defense - Sri Lanka, https://www.defence.lk/Publication/defence_research_and_development (accessed on 1 September 2025) Defence Services Command and Staff College, 'Defence and Security Journal,' 7, 2022, https://dscsc.lk/wp-content/uploads/2023/02/Security-journal-1-1.pdf (accessed on 1 September 2025)

Telecommunications Technology with Foreign Components

Beyond specialized spyware, the hardware backbone of Sri Lanka's telecommunications and internet infrastructure features foreign components that may facilitate intrusion. Over the past two decades, Chinese telecom giants like Huawei and ZTE have been instrumental in building the country's digital infrastructure, providing much of the equipment for Sri Lanka Telecom's ADSL broadband network and Mobitel's 4G networks.[28]

Sajeeth Ahmed, a cybersecurity expert, cautions that these partnerships, given the close ties between Chinese firms and their government, might have introduced hidden "backdoors" enabling unauthorized data access. While no public evidence of specific backdoors in Sri Lanka has surfaced, these concerns mirror global worries around supply-chain security in telecommunications. This raises risks of foreign-made equipment containing hidden vulnerabilities allowing external actors to secretly access or control communication networks. In one anecdote shared by Ahmed, home internet routers in Sri Lanka supplied by Huawei were observed sending unusual "beacon" network signals to unknown external servers, which could potentially be a form of telemetry or a backdoor channel. Such unverified reports contribute to a growing public distrust of foreign technology in critical national networks.

[28] Sanjana Hattotuwa, 'Are Chinese Telecoms acting as the ears for the Sri Lankan government?' Groundviews, 16 February 2012, https://groundviews.org/2012/02/16/are-chinese-telecoms-acting-as-the-ears-for-the-sri-lankan-government/ (accessed on 1 September 2025)

The Impact of Foreign Influence on State Surveillance

The evolution of Sri Lanka's cyber intrusion capabilities cannot be separated from its geopolitical context. Major powers and neighboring countries have, directly or indirectly, shaped Sri Lanka's surveillance toolkit through technology transfer, funding, and diplomatic pressure.

China: China has significantly influenced Sri Lanka's surveillance capabilities by supplying both physical hardware and intellectual expertise. In April 2019, President Sirisena sought assistance from Chinese President Xi Jinping to monitor encrypted platforms like WhatsApp, framing the request as part of an ongoing anti-drug initiative.[29] President Xi reportedly agreed, signaling China's willingness to export its surveillance model. Soon after, Sri Lanka introduced a Chinese-provided facial recognition system at Colombo's Bandaranaike International Airport (BIA) to identify criminal suspects.[30] Although the stated purpose is to identify individuals on watchlists, the system scans all persons passing through the airport - a feature that raises concerns among civil liberties advocates about expanded, indiscriminate citizen monitoring and the potential for function creep.[31] This growing reliance on Chinese surveillance technology highlights the conflict between state security objectives and privacy protections. Furthermore, the Sri Lankan police have tested body-worn cameras, possibly provided by Chinese manufacturers like Hytera, posing questions about whether footage could be transmitted externally without oversight, especially given recent major data breaches in the country.

---

[29] Freedom House, 'Freedom on the Net 2019: Sri Lanka,' Freedom House, 2019, https://freedomhouse.org/country/sri-lanka/freedom-net/2019 (accessed on 1 September 2025)

[30] Xinhua, 'Sri Lanka installs automated face recognition system at main airport to nab criminals,' Xinhua, 6 January 2024, https://english.news.cn/20240106/1a83cdf29bf84d868c85a5dd3790e32d/c.html (accessed on 1 September 2025)

[31] Zulfick Farzan, 'Facial recognition goes full scale at Sri Lanka's main airport,' News 1st, 6 January 2025, https://www.newsfirst.lk/2025/06/06/facial-recognition-goes-full-scale-at-sri-lanka%E2%80%99s-main-airport (accessed on 1 September 2025)

Taylor Braqq, 'Facial recognition is widely adopted in China's airports,' TechWire Asia, 11 April 2018, https://techwireasia.com/2018/04/facial-recognition-is-widely-adopted-in-chinas-airports/ (accessed on 1 September 2025)

These body cams were purchased between 2015 and 2022, with efforts intensifying in the aftermath of the Easter Sunday Attacks, to modernise the police force and enhance public safety. Speaking on this matter, Prasad Perera, a technical expert, stated that Sri Lanka's adoption of new police and surveillance equipment has also occasionally prompted security questions. They further stated that even ostensibly benign tools like police body-worn cameras could pose risks if sourced from vendors susceptible to foreign interference. While body cameras aim to enhance policing transparency, choosing providers carefully is crucial as such devices might inadvertently become channels for data leakage. This highlights the dual risks in external partnerships for surveillance: improved domestic capability but increased vulnerability to foreign espionage.

Israel: Israel's influence has been less overt but equally significant, primarily as a key player in the global market for sophisticated spyware. The secretive 2019 attempt to procure surveillance technology from an unnamed Israeli firm indicated Sri Lanka's interest in acquiring capabilities akin to Pegasus or other advanced telecom interception systems.[32] Prasad, who is familiar with Sri Lanka's cyber surveillance landscape, alleged that government security agencies have shown particular interest not just in acquiring off-the-shelf software but also in adapting Israeli cyber intrusion methods and operational tactics to the local context. Even without confirmed use, the global reputation of Israeli spyware has heightened fears among Sri Lankan journalists and activists, creating a chilling effect on expression.

[32] Freedom House, 'Freedom on the Net 2019: Sri Lanka,' Freedom House, 2019, https://freedomhouse.org/country/sri-lanka/freedom-net/2019 (accessed on 1 September 2025)
Colombo Telegraph, 'Sri Lankan Govt to Spend 6.9 Billion Rupees for Interception Equipment,' Colombo Telegraph, 21 March 2019, https://www.colombotelegraph.com/index.php/sri-lankan-govt-to-spend-6-9-billion-rupees-for-interception-equipment/ (accessed on 1 September 2025)

India: India plays a dual role, supporting digital modernization while simultaneously raising concerns about data sovereignty. A significant example is India's assistance since 2022 to develop Sri Lanka's biometric digital identity system, funded by a substantial grant.[33] The system is based on the Modular Open-Source Identity Platform (MOSIP), an open-source framework inspired by India's Aadhaar system.[34] Darshatha Gamage, a digital rights activist, said that the project sparked controversy among politicians and privacy advocates, who worried that involving Indian firms might risk sensitive personal data being accessed or misused by foreign entities. He also mentioned that Anura Kumara Dissanayake, now President, expressed such fears in 2023 while in the opposition. Although the current administration has given assurances that only local entities will manage the database and that it will be audited by Sri Lanka Computer Emergency Response Team (CERT), the technical specifics of Indian involvement remain opaque, fueling ongoing skepticism.[35]

Perceptions on State Surveillance in Sri Lanka

A recurring theme in Sri Lanka's surveillance narrative is the profound opacity surrounding the state's capabilities. The government rarely discloses what tools it uses for electronic monitoring or how extensively they are deployed. This lack of transparency has bred an environment of suspicion, rumor, and fear, particularly among groups historically targeted, such as journalists, human rights defenders, minority activists, and opposition politicians.

[33] Lanka News Web, 'Sri Lanka to Roll out Digital ID by April 2026 with Indian support,' Lanka News Web, 2 August 2025, https://lankanewsweb.net/archives/105608/sri-lanka-to-roll-out-digital-id-by-april-2026-with-indian-support/ (accessed on 1 September 2025)
Aroonim Bhuyan, 'Sri Lanka's India-funded Digital ID Signals Broader Shift in South-South Tech Cooperation,' ETV Bharat, https://www.etvbharat.com/en/!international/sri-lanka-india-funded-digital-id-signals-broader-shift-in-south-south-tech-cooperation-enn25080303329 (accessed on 1 September 2025)
[34] Ibid
[35] Ibid

This climate of mistrust is not merely anecdotal; it is reflected in the public's behavior. A 2024 analysis of cybercrime in Sri Lanka found that an estimated 61% of all cybercrime incidents go unreported to the authorities.[36] The primary reasons cited include the authorities' perceived inability to take effective action, particularly in cases of online harassment or personal embarrassment, and the belief that certain crimes - such as malware attacks - are too common to warrant a report.[37] This data provides empirical evidence for the consequences of state opacity and a weak rule of law, demonstrating a breakdown in public trust.

Several interviewees for this report admitted uncertainty about the government's exact methods, even as they strongly suspected they were being watched either through phone tapping or digital surveillance. This forces individuals to self-censor. Ashwini Natesan, an expert in Tech Media and Telecommunication Law, noted that information about surveillance tools is not publicly debated in Sri Lanka's Parliament or judiciary, and there is no clear legal framework that lists or limits the technologies law enforcement can use. As a result, many assume a worst-case scenario: if a powerful spyware exists on the global market, the Sri Lankan authorities might have it.

Contributing to this public mistrust is the widespread understanding that intelligence and law enforcement agencies make informal data requests to internet service providers (ISPs) and telecom companies under the pretext of national security. There is scant public data on how frequently this occurs or whether companies resist or comply with these requests within legal boundaries or lack thereof, further cementing the perception of a surveillance state operating beyond the reach of the law.

[36] Maheesha Mudugamuwa, 'Controversial Pegasus spyware: Govt dismisses using the spyware,' The Morning, 24 July 2021, http://www.themorning.lk/controversial-pegasus-spyware-govt-dismisses-using-the-spyware/ (accessed on 1 September 2025)
[37] Ibid

Legal Framework

Sri Lanka's Fractured Cyber Surveillance Framework

Sri Lanka's legal approach to cyber surveillance has evolved through a piecemeal process, resulting in a fractured and inadequate framework built from a combination of outdated statutes and new, issue-specific legislation. While there is broad consensus that surveillance capabilities are necessary to address genuine security threats, particularly given the country's history with civil conflict and terrorism, the existing legal patchwork fails to provide a coherent or comprehensive system of governance. This has created a strategic ambiguity that enables potential overreach, allowing powers intended for legitimate security purposes to be aimed at vulnerable groups in society.

The core challenge in piecing together Sri Lanka’s legislation is the ambiguity between lawful interception for criminal justice purposes, which is covered by specific legislation, and other investigative techniques used for intelligence gathering, which operate in a less defined legal space. This creates a "legality loophole" where the state can circumvent the procedural safeguards of criminal law by framing its surveillance as a national security intelligence operation. This intelligence-driven surveillance operates in a grey area, largely devoid of judicial oversight, a systemic feature that enables potential abuse with little accountability.

Act	Relevant Section(s)	Key Powers Granted	Oversight / Limitations
Sri Lanka Telecommunications Act, No. 25 of 1991[38]	Section 59	Authorizes a telecommunication officer to intercept, monitor, trace, or record calls made for the purpose of causing annoyance (Sri Lanka Telecommunications Act, 1991).	The scope is narrowly defined for "annoyance" calls and does not require a judicial warrant. The Act lacks provisions for broader surveillance and fails to mandate transparency regarding interception requests (Sri Lanka Telecommunications Act, 1991).
Sri Lanka Telecommunications Act, No. 25 of 1991[39]	Section 69	Authorizes the Minister, during a public emergency or in the interest of public safety, to order the interception or censoring of any or all messages (Sri Lanka Telecommunications Act, 1991).	Power is contingent on a public emergency or threat to public safety. It is a ministerial order, not requiring a judicial warrant, and lacks transparency mechanisms.

[38] Sri Lanka Telecommunications Act, No. 25 of 1991, Parliament of the Democratic Socialist Republic of Sri Lanka, https://stepbysteptrade.lk/media/No.25%20of%201991.pdf (accessed on 1 September 2025).
[39] Ibid.

Computer Crimes Act, No. 24 of 2007[40]	Section 18	Permits authorities to intercept electronic communications and access subscriber data during investigations.	Requires judicial authorization (a warrant from a Magistrate). However, it includes a critical exception allowing a police officer to act without a warrant in "urgent situations," with only retroactive court approval required.
Anti-Corruption Act, No. 9 of 2023[41]	Section 58	Empowers investigators from the Commission to Investigate Allegations of Bribery or Corruption to conduct covert monitoring and record communications (Anti-Corruption Act, 2023).	Requires a warrant from the High Court, providing a higher level of judicial oversight compared to other acts. The power is limited to investigations of bribery and corruption (Anti-Corruption Act, 2023).
Online Safety Act, No. 9 of 2024[42]	Section 35	Allows authorities to obtain subscriber and traffic data and compel social media platforms to reveal the identities of anonymous users.	Powers are vested in the Online Safety Commission, whose members are appointed by the President, raising significant concerns about political influence and a lack of judicial independence.

[40] Computer Crimes Act, No. 24 of 2007, Parliament of the Democratic Socialist Republic of Sri Lanka, https://www.icta.lk/icta-assets/uploads/2016/03/ComputerCrimesActNo24of2007.pdf (accessed on 1 September 2025)

[41] Anti-Corruption Act, No. 9 of 2023, Parliament of the Democratic Socialist Republic of Sri Lanka, https://parliament.lk/uploads/acts/gbills/english/6296.pdf (accessed on 1 September 2025)

[42] Online Safety Act, No. 9 of 2024, Parliament of Democratic Socialist Republic of Sri Lanka, https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf (accessed on 1 September 2025)

The Personal Data Protection Act (PDPA): A Step Towards Accountability?

Amidst this fragmented landscape, the passage of the Personal Data Protection Act (PDPA)[43] represents a significant step forward, aimed at aligning Sri Lanka with global privacy standards like the European Union's General Data Protection Regulation (GDPR).[44] Passed in March 2022, the PDPA has established stringent obligations for how personal data is handled both by public and private sector entities.

Most crucially under Section 24, it mandates that organizations conduct Data Protection Impact Assessments (DPIAs) for any high-risk data processing activities, a requirement that would apply to state surveillance operations. This procedural safeguard could, in theory, compel state agencies to formally assess and mitigate the privacy risks of their surveillance programs before implementation.

However, the promise of the PDPA has been severely undermined by considerable implementation delays that have yet to put the law in full force.[45] Experts clarify that these delays are not due to a lack of political will but rather because of bureaucratic obstacles and resistance at the operational ministry level, particularly regarding the funding and staffing of the new Data Protection Authority (DPA). This slow implementation has created a prolonged period of legal uncertainty. Furthermore, legal experts point out that the Act's scope is limited to the protection of "personal data," which is a narrower concept than the broader fundamental right to "privacy".

Critical Deficiencies and Evolving Safeguards

While the system is plagued by profound gaps that leave citizens vulnerable, some important and imperfect safeguards do exist.

---

[43] Personal Data Protection Act, No. 9 of 2022, Parliament of the Democratic Socialist Republic of Sri Lanka, https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf (accessed on 1 September 2025)

[44] Nisali Pieris, 'Data protection legislation in Sri Lanka,' Nithya Partners, https://www.nithyapartners.com/journal/data-protection-legislation-in-sri-lanka (accessed on 1 September 2025)

[45] DataGuidance, 'Sri Lanka - Data Breach,' DataGuidance, 28 August 2022, https://www.dataguidance.com/notes/sri-lanka-data-breach (accessed on 1 September 2025)

Gaps in Oversight and Procedure

The foremost gap is the lack of a single, explicit surveillance law, particularly one that governs and addresses the intelligence-driven operations for national security. This legal void is compounded by the absence of a dedicated, independent oversight body. While Sri Lanka has a parliamentary Sectoral Oversight Committee on National Security, its function is political and legislative rather than judicial or technical and it does not authorize or review specific surveillance warrants in real-time.[46] This stands in stark contrast to international best practices, which call for independent, often judicial, bodies to oversee state surveillance to prevent abuse.[47]

This institutional gap is worsened by what a former head of a government institution describes as a "lacuna" or gap in Standard Operating Procedures (SOPs) for law enforcement. While there were internationally-supported efforts to draft SOPs for interception activities, the process has been stalled due to personnel transfers and a lack of institutional continuity, leaving law enforcement without clear, rights-respecting guidelines.

Existing Safeguards and Avenues for Redress

Despite these significant gaps, there are some notable checks on state power:

- **The Budapest Convention:** As a state party to this international cybercrime convention, Sri Lanka is compelled under international law (Article 15) to adhere to human rights and rule-of-law safeguards when conducting intrusive investigations.

- **Constitutional Remedies:** In the absence of a fully operational PDPA, constitutional protections provide a crucial safeguard. Sri Lanka's Supreme Court has a history of judicial activism, and experts note a resurgence of this activism since 2016-17, providing a vital check against potential overreach.

---

[46] Sectoral Oversight Committee on National Security, 'Report of the Proposals for Formulation and Implementation of relevant laws required to ensure National security that will eliminate New Terrorism and extremism by strengthening friendship among Races and Religions,' Parliament of Sri Lanka, 19 February 2020, https://www.parliament.lk/uploads/comreports/1582610584075624.pdf (accessed on 1 September 2025)

[47] Freedom Online Coalition, 'Guiding Principles on Government Use of Surveillance Technologies,' Freedom Online Coalition, March 2023, https://freedomonlinecoalition.com/guiding-principles-on-government-use-of-surveillance-technologies/ (accessed on 1 September 2025)

Implications for Society

This ambiguous and high-risk legal environment has tangible consequences for different sectors of Sri Lankan society.

Civil Society and Journalists: For activists and reporters, the legal ambiguity creates a palpable climate of caution and self-censorship.[48] The fear is that "national security" can be used as a pretext to target dissent, a concern rooted in the past misuse of laws like the Prevention of Terrorism Act.[49]

The Private Sector: Telecommunication companies navigate a precarious position. According to experts, their licensing conditions require them to comply with government requests for data. This places them in a difficult bind when they receive requests from intelligence agencies that may lack a clear court order, pitting their licensing obligations against their duties to protect user privacy.

[48] Freedom House, 'Freedom on the Net 2024: Sri Lanka,' Freedom House, 2025 https://freedomhouse.org/country/sri-lanka/freedom-net/2024 (accessed on 1 September 2025)

[49] Adayaalam Centre for Policy Research, 'A phantom that is Real: Persisting Culture of Surveillance and Intimidation in the North-East, Adayaalam Centre for Policy Research, February 2025, https://adayaalam.org/wp-content/uploads/2025/05/A-Phantom-that-is-Real_-Persisting-Culture-or-Surveilance-and-Intimidation-in-the-NorthEast.pdf (accessed on 1 September 2025)

Recommendations

Forging a Rights-Respecting Framework

The preceding analysis reveals significant gaps in Sri Lanka's legal, institutional, and societal frameworks for governing cyber intrusion and surveillance. To balance legitimate national security needs with the fundamental rights of citizens, a multi-pronged approach is necessary. The following recommendations are based on expert interviews, global best practices, and a contextual analysis of Sri Lanka's evolving digital landscape. The path to transparency and accountability in Sri Lanka's spyware landscape requires more than just legislative tweaks; it demands a holistic, "whole-of-society" strategy where legal, institutional, and public awareness reforms are interconnected and mutually reinforcing. A new law will be ineffective if the public does not trust the institutions meant to enforce it, and those institutions cannot succeed without the capacity and rights-based training to implement it properly.

Strengthen Legal and Policy Frameworks

A robust legal architecture is the bedrock of a rights-respecting surveillance regime. Sri Lanka must move from its current fragmented approach to a consolidated, modern framework.

- **Enact a Consolidated Surveillance Law:** Parliament should draft and enact a single, comprehensive law governing all forms of state surveillance. This legislation must explicitly incorporate the international human rights principles of legality, necessity, and proportionality. It should clearly define the scope, limitations, and procedures for both targeted and incidental data collection, explicitly prohibiting mass surveillance.

- **Mandate Judicial Pre-Authorization:** The new surveillance law must require prior authorization from an independent judicial body for any intrusive surveillance measure. This would close existing loopholes, such as the "urgent situation" exception in the Computer Crimes Act (No. 24 of 2007), and ensure that surveillance is not initiated on the sole discretion of law enforcement or intelligence agencies.

- **Repeal and Reform the Online Safety Act:** The Online Safety Act (No. 9 of 2024) should be immediately repealed. Its vague definitions of "false" and "harmful" speech and the creation of a politically appointed commission with censorship powers are incompatible with democratic principles and freedom of expression.[50] Any future legislation aimed at addressing online harms must be narrowly tailored and place adjudicative power with the independent judiciary, not a political body.

- **Expedite Full Implementation of the PDPA:** The government must prioritize the full implementation of the Personal Data Protection Act (No. 9 of 2022). This includes providing the necessary funding and staffing to make the Data Protection Authority (DPA) fully operational and immediately enacting the specific regulations (Schedule IV) governing the processing of data for law enforcement and national security purposes.

Improve Oversight, Transparency, and Accountability

Effective oversight is crucial to prevent the abuse of surveillance powers and build public trust.

- **Establish an Independent Oversight Body:** Sri Lanka should create an independent, multi-stakeholder oversight body with the legal authority and technical expertise to supervise all state surveillance activities. This body should be empowered to conduct audits, review the legality and proportionality of surveillance warrants, and investigate public complaints. Its membership should include representatives from the judiciary, legal profession, human rights commissions, and technical experts.

- **Mandate Transparency in Procurement and Use:** All procurement of surveillance technology must be subject to public procurement laws and parliamentary oversight along with stricter controls on private intermediaries involved in government procurements. The government should be required to publish periodic transparency reports detailing the aggregate number of interception orders requested, granted, and denied, thereby providing a measure of public accountability.

[50] ICJ, 'Sri Lanka: Proposed Online Safety Bill would be an assault on freedom of expression, opinion and information,' International Commission of Jurists, 29 September 2023, https://www.icj.org/sri-lanka-proposed-online-safety-bill-would-be-an-assault-on-freedom-of-expression-opinion-and-information/ (accessed on 1 September 2025)

- **Enhance Accountability and Redress Mechanisms:** Individuals who are unlawfully targeted by surveillance must have access to effective legal remedies. This includes the ability to file fundamental rights petitions, lodge complaints with the DPA, and seek compensation for damages. Legal and disciplinary consequences must be established for officials who misuse surveillance authorities.

- **Create SOPs :** One concrete proposal to enhance oversight is the creation of a "generalized checklist" for all national-level technological interventions that involve cyber intrusion, similar to how an environmental impact assessment is required for development projects. Such a checklist would need to be passed before a project could be implemented, ensuring that privacy and human rights considerations are addressed from the outset.

Engage Civil Society and Promote Public Participation

A resilient digital society requires an informed and engaged citizenry.

- **Launch Targeted Public Awareness Campaigns:** Drawing on the findings that 61% of cybercrimes go unreported due to mistrust and lack of awareness,[51] the government, in partnership with civil society organizations, should launch sustained public education campaigns. These campaigns should focus on the most prevalent cyber threats, such as phishing and online harassment, and provide clear, accessible information on secure digital practices and the official channels for reporting crimes.

- **Establish a Multi-Stakeholder Advisory Group:** A permanent multi-stakeholder advisory group on digital rights should be formed to consult on all future legislation and policies related to surveillance, data protection, and online speech. This group should include representatives from civil society, academia, the technology industry, and the legal community to ensure that diverse perspectives inform policy-making.

[51] Heshan Maduranga, 'Cybercrime Analysis – Sri Lanka,' Cardiff Metropolitan University, 4 May 2023, https://www.researchgate.net/publication/378336517_Cybercrime_Analysis_-_Sri_Lanka (accessed on 1 September 2025)

Build Institutional and Technical Capacity

Regulation and oversight are only effective if the relevant institutions have the capacity to implement them.

- **Prioritize Defensive Cybersecurity:** A strategic shift in funding and focus is needed, moving away from the disproportionate investment in offensive intrusion tools towards strengthening the nation's defensive cybersecurity infrastructure. This aligns with the stated goals of the National Cyber Security Strategy (2025-2029) and addresses the critical weaknesses identified by the National Cyber Security Index.[52]
- **Provide Rights-Based Training:** Capacity-building initiatives for law enforcement, intelligence agencies, and the judiciary must include mandatory, comprehensive training on international human rights law, the principles of necessity and proportionality, and the proper, court-admissible handling of digital evidence.
- **Invest in Capacity Building for Government Agencies:** A significant barrier to effective implementation is the lack of a sufficient knowledge pool within government agencies to manage and troubleshoot advanced surveillance technologies.

By adopting these integrated recommendations, Sri Lanka can transition from a reactive, fragmented approach to cyber surveillance to one that is legally coherent, ethically grounded, transparently managed, and publicly accountable. This shift will not only safeguard civil liberties but also foster the public trust and digital innovation essential for long-term national security and prosperity.

[52] Heshan Maduranga, 'Cybercrime Analysis – Sri Lanka,' Cardiff Metropolitan University, 4 May 2023, https://www.researchgate.net/publication/378336517_Cybercrime_Analysis_-_Sri_Lanka (accessed on 1 September 2025)

Conclusion

Sri Lanka's surveillance trajectory reveals a troubling pattern where national security continues to serve as a convenient and elastic justification for expanding state power with minimal transparency and accountability. From wartime intelligence operations to post-war cyber espionage and spyware acquisitions, surveillance has become a normalized feature of governance rather than an extraordinary measure. The absence of comprehensive legislation, and independent oversight has allowed this practice to evolve in the shadows, often targeting journalists, civil society, and political opponents.

At the same time, the rapid digitalization of governance and public services, from biometric identity systems to online data exchanges, has blurred the boundaries between technological modernization and state control. Without a fully implemented Personal Data Protection Act and clear institutional checks, these initiatives risk deepening existing vulnerabilities rather than strengthening citizen trust. The combination of foreign technological influence, weak domestic safeguards, and limited public awareness has produced a surveillance environment that is both sophisticated and opaque.

Ultimately, the challenge for Sri Lanka lies not only in reforming its surveillance laws but in reimagining the relationship between the state, technology, and the individual. Ensuring accountability, transparency, and human rights in the digital age demands a shift from secrecy to oversight, from control to protection, and from reactive governance to proactive rights-based policy.

Works Cited

Ada Derana. “CBK reveals why she used Viber to topple MR.” Ada Derana, January 20, 2015, https://www.adaderana.lk/news.php?nid=32243

Adayaalam Centre for Policy Research. “A phantom that is real: Persisting culture of surveillance and intimidation in the North-East.” Tamil Guardian, February 2025, https://www.tamilguardian.com/content/new-report-details-sri-lanaksas-phantom-culture-surveillance-and-intimidation-north-east

Anti-Corruption Act, No. 9 of 2023, Parliament of the Democratic Socialist Republic of Sri Lanka. https://parliament.lk/uploads/acts/gbills/english/6296.pdf

Bhuyan, Aroonim. “Sri Lanka's India-funded digital ID signals broader shift in South-South tech cooperation.” ETV Bharat, August 3, 2025, https://www.etvbharat.com/en/!international/sri-lanka-india-funded-digital-id-signals-broader-shift-in-south-south-tech-cooperation-enn25080303329

Braqq, Taylor. “Facial recognition is widely adopted in China’s airports.” TechWire Asia, April 11, 2018, https://techwireasia.com/2018/04/facial-recognition-is-widely-adopted-in-chinas-airports/

Centre for Defence Research & Development, https://crd.lk/
Centre for Defence Research & Development. “Satellite & Surveillance Wing.” Centre for Defence Research & Development https://crd.lk/wingSattelite%20&%20Surveillance%20Wing

Colombo Telegraph. “Sri Lankan Govt to Spend 6.9 Billion Rupees for Interception Equipment.” Colombo Telegraph, March 21, 2019, https://www.colombotelegraph.com/index.php/sri-lankan-govt-to-spend-6-9-billion-rupees-for-interception-equipment/

CSL CER. “Initial discussion on the proposed Memorandum of Understanding (MoU) between the University of Ruhuna (UoR) and the Centre for Defence Research and Development (CDRD).” China-Sri Lanka Joint Center for Education and Research, May 20, 2025, https://cslcer.ruh.ac.lk/newspost.php?post=20

DataGuidance. “Sri Lanka - Data Breach.” DataGuidance, February 22, 2024 https://www.dataguidance.com/notes/sri-lanka-data-breach

Defence Services Command and Staff College. Defence and Security Journal, 7, (2022). (https://dscsc.lk/wp-content/uploads/2023/02/Security-journal-1-1.pdf)

e-Governance Academy. “National Cyber Security Index: Sri Lanka.” National Cyber Security Index, January 24, 2023, https://ncsi.ega.ee/

EconomyNext. “Sri Lanka cabinet approves second 5-year cyber security strategy.” EconomyNext, July 15, 2025, https://economynext.com/sri-lanka-cabinet-approves-second-5-year-cyber-security-strategy-230812/

Farzan, Zulfick. “Facial recognition goes full scale at Sri Lanka’s main airport.” News 1st, January 6, 2025, https://www.newsfirst.lk/2025/06/06/facial-recognition-goes-full-scale-at-sri-lanka%E2%80%99s-main-airport

Forbidden Stories. “The Pegasus Project.” Forbidden Stories, 2021, https://forbiddenstories.org/about-the-pegasus-project/

Freedom House. “Freedom on the Net 2014: Sri Lanka.” Freedom House, 2014, https://www.refworld.org/reference/annualreport/freehou/2014/en/102727

Freedom House. “Freedom on the Net 2019: Sri Lanka.” Freedom House, 2019, https://freedomhouse.org/country/sri-lanka/freedom-net/2019

Freedom House. “Freedom on the Net 2020: Sri Lanka.” Freedom House, 2020 https://freedomhouse.org/country/sri-lanka/freedom-net/2020

Freedom House. “Freedom on the Net 2024: Sri Lanka.” Freedom House, 2025, https://freedomhouse.org/country/sri-lanka/freedom-net/2024

Freedom Online Coalition. “Guiding principles on government use of surveillance technologies.” Freedom Online Coalition, March 9, 2023 https://freedomonlinecoalition.com/guiding-principles-on-government-use-of-surveillance-technologies/

Hattotuwa, Sanjana. “Are Chinese Telecoms acting as the ears for the Sri Lankan government?” Groundviews, February 16, 2012, https://groundviews.org/2012/02/16/are-chinese-telecoms-acting-as-the-ears-for-the-sri-lankan-government/

Hattotuwa, Sanjana. “Hacking the hackers: Surveillance in Sri Lanka revealed.” GroundViews, July 15, 2015, https://groundviews.org/2015/07/15/hacking-the-hackers-surveillance-in-sri-lanka-revealed/

Hern, Alex. “Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim.” The Guardian, July 6, 2015, https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

HRW. “Sri Lanka: Reject New Counterterrorism Bill.” Human Rights Watch, April 7, 2023, https://www.hrw.org/news/2023/04/07/sri-lanka-reject-new-counterterrorism-bill

Hytera. “Hytera Body Camera.” Hytera, https://www.hytera.com/en/product-new/body-worn-camera/body-worn-camera-solution.html

ICJ. “Sri Lanka: Proposed Online Safety Bill would be an assault on freedom of expression, opinion and information.” International Commission of Jurists, October 2, 2023, https://www.icj.org/sri-lanka-proposed-online-safety-bill-would-be-an-assault-on-freedom-of-expression-opinion-and-information/

Kaldani, Tamar, and Zeev Prokopets. “Pegasus and the surveillance of journalists.” Council of Europe, April 2022, https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8

Kumarasiri, Hon. J.M. Ananda. “Report of the Select Committee of Parliament to look into and report to Parliament on the Terrorist Attacks that took place in different places in Sri Lanka on 21st April 2019.” Parliament of Sri Lanka, October 23, 2019, https://www.parliament.lk/uploads/comreports/sc-april-attacks-report-en.pdf

Lanka News Web. “Sri Lanka to roll out Digital ID by April 2026 with Indian support.” Lanka News Web, August 2, 2025, https://lankanewsweb.net/archives/105608/sri-lanka-to-roll-out-digital-id-by-april-2026-with-indian-support/

Maduranga, Heshan. “Cybercrime Analysis – Sri Lanka.” Cardiff Metropolitan University, May 4, 2023, https://www.researchgate.net/publication/378336517_Cybercrime_Analysis_-_Sri_Lanka

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Petranto, and Sarah McKune. “Pay No Attention to the Server Behind the Proxy: Mapping FinFisher’s Continuing Proliferation.” The Citizen Lab, October 15, 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

Ministry of Defence. “Defence Research and Development Projects.” Ministry of Defense - Sri Lanka, https://www.defence.lk/Publication/defence_research_and_development

Ministry of Technology. “National Cyber Security Strategy of Sri Lanka (2025 - 2029).” Sri Lanka CERT, https://www.cert.gov.lk/wp-content/uploads/policies/National_Cyber_Security_Strategy_of_Sri-Lanka.pdf

Mudugamuwa, Maheesha. “Controversial Pegasus spyware: Govt dismisses using the spyware,” The Morning, July 14, 2021, https://www.themorning.lk/controversial-pegasus-spyware-govt-dismisses-using-the-spyware/

Nithya Partners. “Data protection legislation in Sri Lanka.” Nithya Partners, 2022, https://www.nithyapartners.com/journal/data-protection-legislation-in-sri-lanka

NSBM Green University. “NSBM extends MoU with Centre for Defence Research and Development.” NSBM Green University, November 1, 2023, https://www.nsbm.ac.lk/nsbm-extends-mou-with-centre-for-defence-research-and-development/

Parliament of Sri Lanka. “Sectoral Oversight Committee on National Security.” Parliament of Sri Lanka, https://www.parliament.lk/uploads/comreports/1582610584075624.pdf

Patrawala, Fatema. “Is China's facial recognition powered airport kiosks an attempt to invade privacy?” Packt, March 26, 2019, https://www.packtpub.com/en-us/learning/tech-news/chinas-facial-recognition-powered-airport-kiosks-an-attempt-to-invade-privacy?

Personal Data Protection Act, No. 9 of 2022, Parliament of the Democratic Socialist Republic of Sri Lanka.

Samarkoon, Charya, and Bhavani Foneska. “Right to Privacy in Sri Lanka.” Center for Policy Alternatives, September 2020, https://www.cpalanka.org/wp-content/uploads/2020/09/Discussion-Paper-Right-to-Privacy-updated-draft-4-1.pdf

Sectoral Oversight Committee on National Security, “Report of the Proposals for Formulation and Implementation of relevant laws required to ensure National security that will eliminate New Terrorism and extremism by strengthening friendship among Races and Religions,” Parliament of Sri Lanka, February 19, 2020, https://www.parliament.lk/uploads/comreports/1582610584075624.pdf

Sri Lanka CERT CC. “Annual Report 2021.” Sri Lanka Computer Emergency Readiness Team Coordination Centre, January 31, 2023, https://www.cert.gov.lk/wp-content/uploads/annual_reports/2021_english.pdf

Sri Lanka Telecommunications Act, No. 25 of 1991, Parliament of the Democratic Socialist Republic of Sri Lanka.

Tamil Guardian. “Sri Lankan defence secretary tapped murdered journalist’s phone.” Tamil Guardian, November 9, 2016, https://www.tamilguardian.com/content/sri-lankan-defence-secretary-tapped-murdered-journalist%E2%80%99s-phone

The Sunday Morning. (2021, July 25). Controversial Pegasus spyware: Govt dismisses using the spyware. The Morning. http://www.themorning.lk/controversial-pegasus-spyware-govt-dismisses-using-the-spyware/

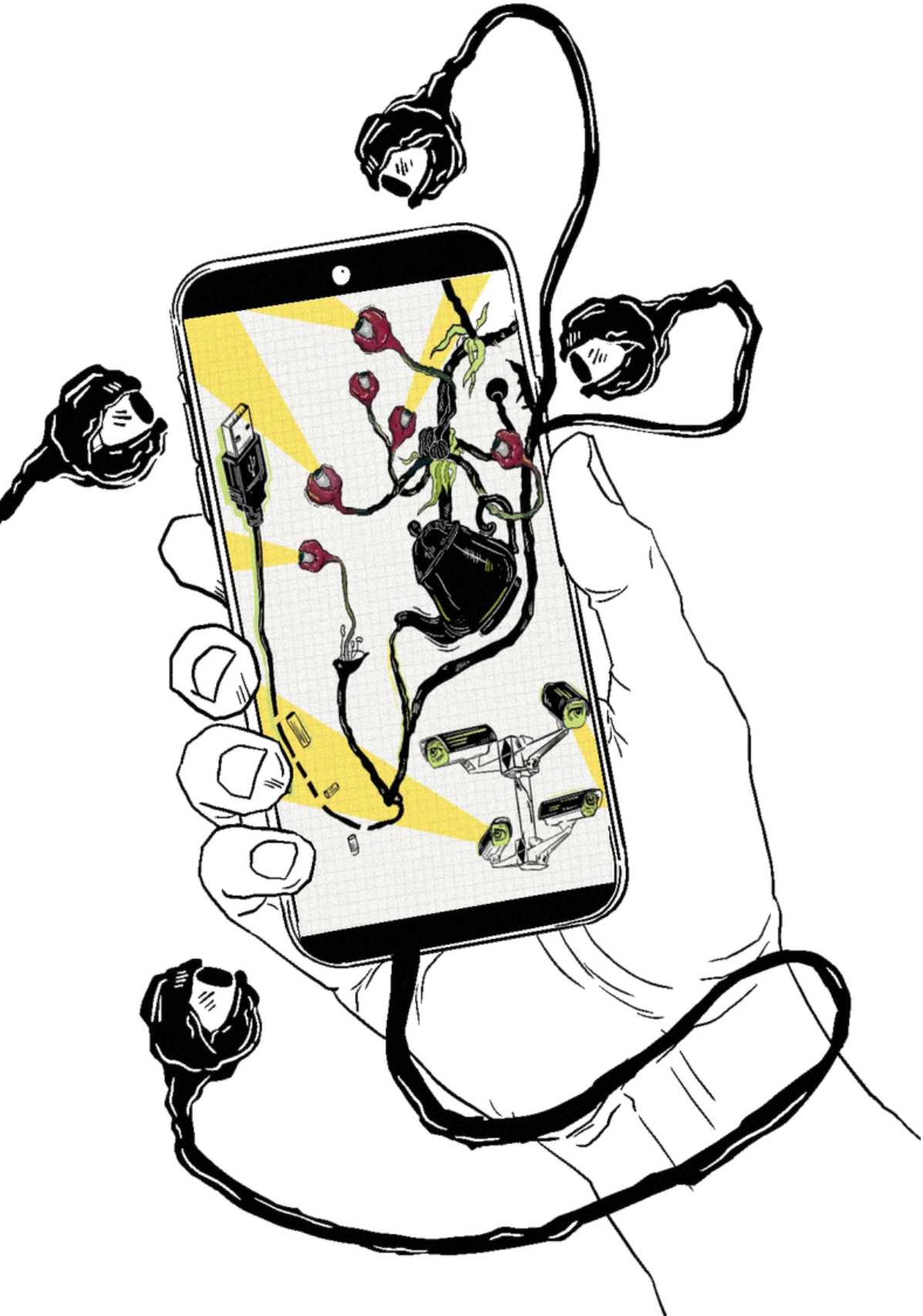
United Nations. “The right to privacy in the digital age.” United Nations High Commissioner for Human Rights, August 4, 2022, https://undocs.org/A/HRC/51/17

WikiLeaks. (2015, July 8). “Hacking Team email archives related to Sri Lanka.” WikiLeaks, July 8, 2015, https://wikileaks.org/hackingteam/emails/emailid/593346

Xinhua. “Sri Lanka installs automated face recognition system at main airport to nab criminals.” Xinhua, January 6, 2024, https://english.news.cn/20240106/1a83cdf29bf84d868c85a5dd3790e32d/c.html

ANALYSIS & CONCLUSION

Chapter 5



Having done a detailed analysis of how the surveillance economy operates in each country, liberties can be taken to discuss what this means for the Indian subcontinent as a whole and for the global market of surveillance tools that have grown profitable on the backs of Global South markets taking advantage of negligent governments.

While the notable lack of government transparency – which varies from country to country – limits comparative research, it's clear that surveillance in the context of growing and mid-tier economies such as Pakistan, India, Bangladesh and Sri Lanka has many similarities, especially given the region's shared past with British colonialism and dysfunctional political regimes. But where these similarities can create common ties, it also creates latent differences. Countries appear to vary in their respective procurement and harmful deployment of surveillance technologies. Accounting for these variations, we have ranked these four countries in order of relative "safeness", specifically in the context of surveillance and its accompanying dangers to civil liberties, based on scores graded by our local experts.

In an attempt to map out a rough ranking of most to least safe countries in South Asia, specifically in the context of surveillance and its accompanying dangers to civil liberties, we asked local experts to grade their respective countries.

Countries were ranked on the basis of a three-part index: (i) the extent to which states declare and/or are reported to have procured surveillance technology, (ii) whether or not states have legal structures in place to deal with human rights violations in the context of surveillance, and (iii) the harmful impact surveillance technologies, alongside larger encroachment of rights, have had on citizens and their civil liberties. These categories were established based on the research conducted under the four case studies - common themes were drawn out and the findings for each country were compared and ranked.. While each category on its own can inform individuals enough about how technologies and entire populations are being monitored, tracked, and exploited, a combination of all three presents a clear hierarchy among the four countries, notwithstanding the general pervasiveness of surveillance and lack of government transparency across the region

Surveillance Technology Transparency

An important aspect of defining state strictness when it comes to surveillance is looking at procurement patterns, inasmuch as they are publicly available. According to the Open Government Partnership (OGP), defense spending or procurement processes that lack transparency are, by extension, free of any oversight whether by institutions or citizens themselves, making it susceptible to inefficiencies, exploitation, and/or unlawful expenditures.[1] Especially vulnerable to undemocratic processes such as this are countries in the Global South – those subjected to colonialism, political instability, and civil conflict, all the while being governed by poorly implemented laws and a weak judicial system.

Drawing from the preceding country reports, it's evident that the Indian subcontinent is a victim of limited public information, especially in the context of government spending. Information that should in practice be accessible by the public as a part of their right to information – an act present in all legal structures across South Asia – is more often than not kept secret under the pretense of security or sensitivity. In Bangladesh and Sri Lanka, for example, researchers found it extremely difficult to find public information directly tying the government to the procurement of sophisticated surveillance technologies in recent years, such as Pegasus, but were able to piece together circumstantial information/evidence that alleges the use of such tools.

[1] Open Government Partnership, 'Defense and Security: Defense Spending, Procurement Transparency and Oversight,' Open Government Partnership, https://www.opengovpartnership.org/open-gov-guide/defense-and-security-defense-spending/#toc_2 (accessed on 1 September 2025)

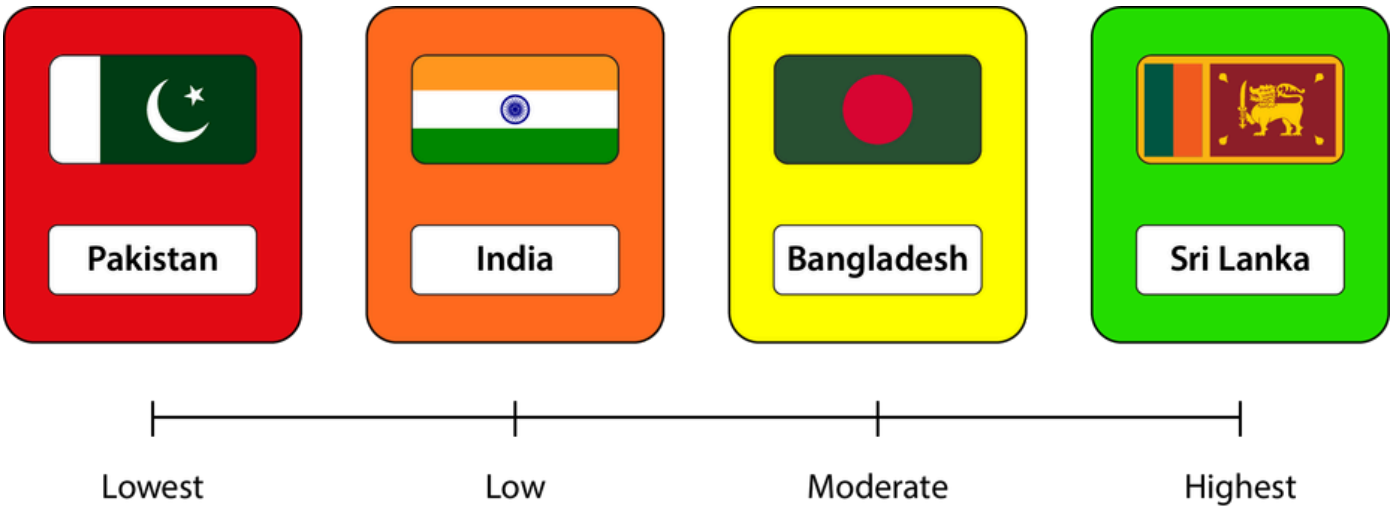
Alternatively, while Pakistan and India are equally limited in their own public records on government procurements, information on their surveillance arsenal can be pieced together through the efforts of international watchdogs and investigators such as Amnesty International, who using in-depth, insider information, have over the years gained crucial intel on surveillance dealings within the countries. As described in detail in each country chapter, Pakistan and India have, in as little as the past 6 months, been exposed to acquiring tools from highly problematic companies such as NSO Group and Intellexa and using them in undemocratic, illegal ways against citizens.

Either way, complete to partial transparency can allow crucial actors such as journalists, civil society organizations, as well as the judiciary to probe into how the government allocates its taxpayers money, what equipment it's investing in and for what purposes. Privacy International (PI), a leading non-profit organization in the realm of digital rights, has pointed out that openness about a government's spending, especially when building a surveillance ecosystem, helps the public "develop an understanding of the necessity and lawfulness..." of its application.[2]

To determine levels of transparency and openness within our region of interest, experts were asked to rank their respective countries based on the relative transparency of the government's surveillance technology procurement process and especially how easily they can find information on such procurement patterns. While all experts say that their states have not been open about their dealings with cyber surveillance vendors, each country had varying degrees of said transparency. Pakistan ranks at the bottom as the least transparent when it comes to sharing information on defense and law enforcement-related expenditure, with India close behind. Experts from Bangladesh and Sri Lanka placed their countries higher in the ranking, determining them to be more open and transparent than their larger counterparts in the region.

[2] https://privacyinternational.org/our-demands/transparency

Legal Protections



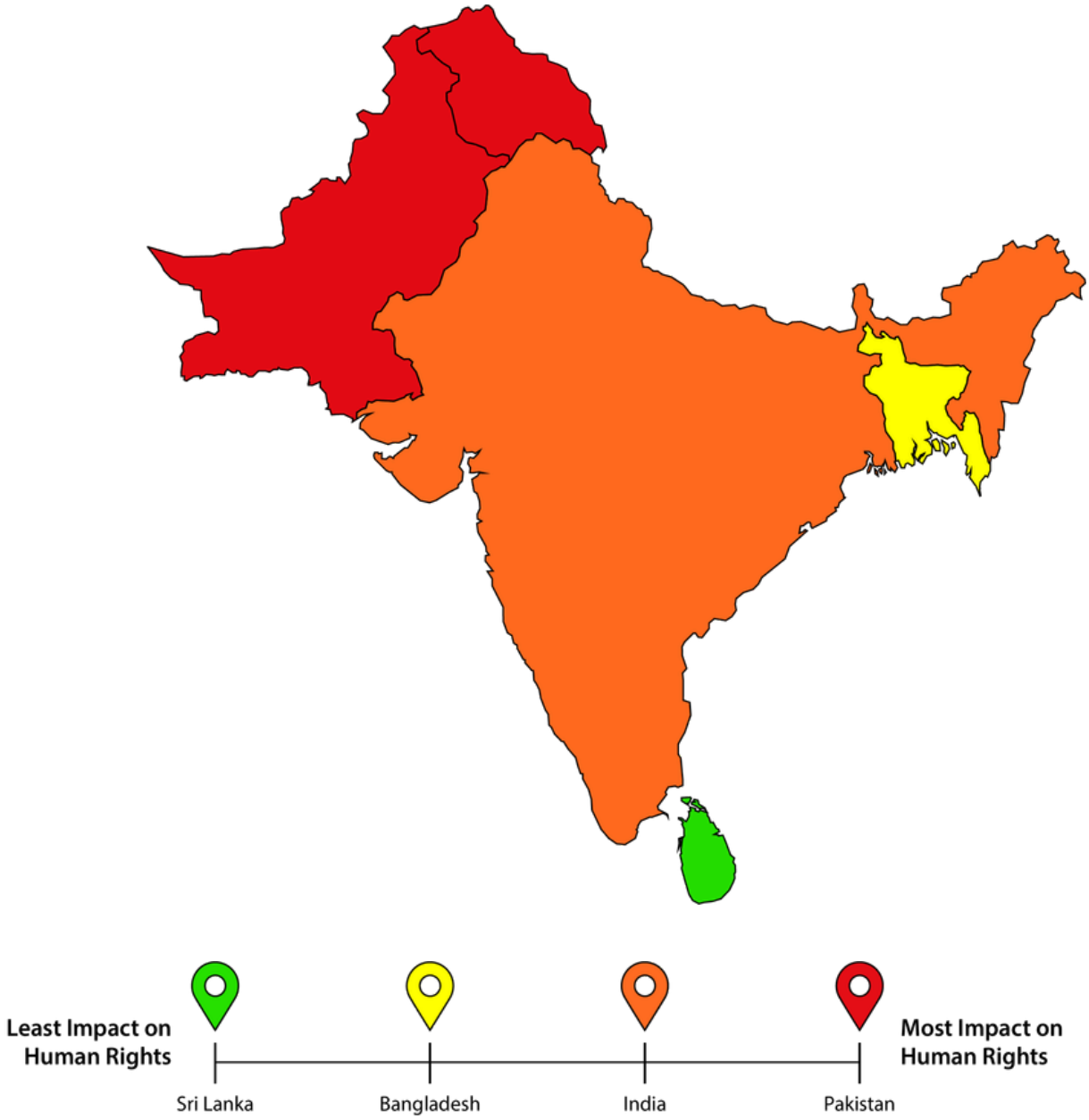
With legislature, and the judiciary by extension, acting as a check and balance for any injustices carried out by the state, the structure and content of a country's laws becomes imperative in the face of newer challenges such as the deployment of cyber surveillance technologies for undemocratic reasons. Legal protections provided by the law to the citizens of a country alongside a judiciary that acts in the interest of the people and against the state as an entity, are a vital indicator for just how safe, remedial and protective a country is when it comes to the common good rather than individual gain.

In our chapters, great detail was given to the legislative makeup of each country and how laws in theory or on paper don't always translate into practical and concrete remedies, especially when combined with a judiciary that lacks the independent power to stand up against pseudo-authoritarian governments. Rules and regulations in the South Asian region find their roots in colonial laws implemented by the British in pre-partition times and though tweaks have been made along the way, most laws still mimic political structures common to colonialism (i.e. authoritarianism).

Most research done and shown by experts in the country chapters shows that the judiciary more often than not acts as a stroke of justice, outlining case laws and precedents that help establish how laws should be applied and implemented. In Pakistan, for instance, legal proceedings in the 1980s from high-profile cases surrounding politicians set the landscape for what was or wasn't allowed when collecting information against the opposition. Similarly, in India, recent proceedings in the Pegasus case show hope that the judicial system can function independently to benefit citizens.

On the other hand, legislation can just as easily be manipulated by the state to reflect its own agenda. The introduction of draconian laws such as PECA in Pakistan and the Digital Security Act in Bangladesh are evidence of the fact that control over the legal mechanism of a country is control over its people. To this effect, to help identify how proactive a government's laws are in the South Asian region, experts were asked questions pertaining to the legislative structure, including whether the government has excessive control over privacy laws and if oversight fails to operate in a free, fair and independent manner, amongst other questions. With all experts in the South Asian regions responding in the affirmative, it’s clear to see how governments in the guise of legal protections are subjecting citizens' right to privacy and freedom of expression. Minor variations were seen when asking how excessive of a control the state has on laws in the country with Pakistan being ranked at the top (a lot of control) and Sri Lanka at the bottom (moderate control).

Impact on Human Rights



The third and most critical component of our index assesses the direct impact of surveillance practices on civil liberties and human rights. While surveillance procurement patterns and legal structures provide insight into state capacity and safeguards, the human rights index reflects lived realities relating to arrests, intimidation, chilling effects, censorship, political manipulation and privacy violations. Based on expert assessments across the four case studies, this ranking reflects the degree to which surveillance technologies have translated into tangible harm to citizens, especially journalists, activists, opposition leaders and marginalized communities. It is important to note here that this ranking in particular relies on information publicly available either in confirmed news reports or analyses from human rights organizations.

Sri Lanka ranks highest in relative safety in terms of direct human rights impact. While the country has pursued spyware procurement and deployed surveillance during periods of unrest, the scale and systematic targeting appear comparatively limited. The passage of the Personal Data Protection Act and reform rhetoric under new administrations provide some institutional restraint. However, this ranking is relative. Surveillance during the civil war, monitoring of protest movements such as the Aragalaya, and continued intelligence presence in minority regions show that risks remain. Yet, compared to its regional counterparts, Sri Lanka demonstrates comparatively lower systemic and sustained digital repression.

India ranks second in terms of impact. The Pegasus disclosures and Apple threat notifications revealed the targeting of journalists, lawyers and opposition politicians, which reflects serious breaches of privacy and democratic norms. However, India's ranking reflects the presence of judicial contestation and institutional pushback. The Supreme Court's involvement in Pegasus-related litigation, constitutional recognition of privacy and ongoing public debate create friction within the system. While harm has occurred, institutional resistance tempers its overall impact relative to Bangladesh and Pakistan.

Bangladesh ranks third, reflecting more systematic and politically embedded use of surveillance tools. Thousands of cases under the Digital Security Act and related laws, widespread arrests of journalists and activists and documented surveillance expansion during election cycles illustrate how cyber intrusion technologies have intersected directly with political consolidation. The chilling effect is significant and measurable, with self-censorship in media institutions and documented targeting of critics. Surveillance in Bangladesh has not only enabled monitoring, but it has also facilitated detention, disappearance and direct suppression of dissent.

Pakistan ranks lowest, indicating the highest level of impact on human rights among the four countries. The combination of warrantless interception systems, expanded administrative data access, limited oversight and repeated misuse against political opponents creates a high-risk environment. The impact includes systematic targeting of opposition politicians, audio leak scandals, monitoring of journalists and activists, and weak judicial enforcement of privacy protections. There is also the absence of an effective data protection law and the rise of cases where the use of the Prevention of Electronics Crimes Act (2016) has led to restricting freedoms online. Both surveillance capacity and weak oversight converge, and human rights harms have become more normalized than ever before. Pakistan, therefore, represents the most concerning case in terms of direct and sustained rights impact.

Conclusion

When all three indices are considered together relating to surveillance technology transparency, legal protections and impact on human rights, a comprehensive and cumulative regional picture emerges.

- Sri Lanka consistently ranks highest across all three categories, making it comparatively the safest within this index framework, though not free from risk.
- India ranks second overall, supported by stronger constitutional protections but weakened by executive opacity and spyware revelations.
- Bangladesh ranks third, reflecting moderate transparency but significant political use of surveillance laws and tools.
- Pakistan ranks lowest across all three indices, demonstrating the most concerning convergence of opaque procurement, weak legal safeguards and high human rights impact.

This cumulative ranking suggests that the severity of surveillance-related harm is closely tied to two structural factors: the degree of transparency in procurement and oversight, and the strength, or fragility, of legal protections. Where procurement processes are opaque and oversight mechanisms are weak, surveillance technologies are more likely to be misused. Across the Indian subcontinent, surveillance capacity has expanded at a pace that has consistently outstripped legal reform and institutional accountability. As a result, the region has become an increasingly attractive market for global surveillance vendors, particularly in governance environments where regulatory safeguards remain underdeveloped or easily circumvented.

The findings make clear that no country in South Asia can claim a fully rights-respecting surveillance framework. Even the highest-ranked state exhibits structural vulnerabilities that could enable abuse under different political conditions. And while nation-states themselves hold a large chunk of the responsibility for consequences from dealing with violations from surveillance technologies, there is no doubt that foreign third party actors are taking advantage of the region and its politically unstable environment. Opaque international surveillance technology markets with limited regulations that are continuously exploited by companies in the West (where these technologies are being developed),profiting off of legislative blind spots in international law.

The gradation in rankings offers a valuable policy roadmap for stronger and clearer legal frameworks, judicial independence that can meaningfully mitigate harm, and transparency in procurement, which reduces the likelihood of abuse. It has already been seen that political instrumentalization of surveillance technologies dramatically amplifies their human rights impact in the region, particularly in the politically volatile states of South Asia.

Ultimately, this index does more than rank countries; it reveals how surveillance ecosystems can either constrain state power or facilitate democratic erosion. Without coordinated domestic reform, robust oversight mechanisms and stronger international regulation of the spyware market, the region risks further normalizing digital repression as a routine feature of governance in South Asia.

Appendix

The following questionnaire was used to build an index for our study. The questionnaire was designed to gather information from country experts in Pakistan, India, Bangladesh and Sri Lanka regarding the cyber-surveillance landscape in South Asia in 3 parts. The questionnaire was sent over to participants via email and all responses were treated confidentially. The data collected was used solely for research and analysis purposes.

Cyber-Surveillance Index Questionnaire

As a part of our final chapter for the scoping study that each of you have conducted in your respective studies, we are conducting a combined analysis of all the insights and findings you have described in your drafts. To that effect, we would like to invite you to answer this short questionnaire.

Given your expertise and the extensive research you have conducted for this study, we believe you are in the best position to determine how strict or open your countries are specifically in the context of the surveillance landscape. Each country will be judged and ranked on the basis of three parts:

- The legislation they do (or don't) have in place
- The proliferation of surveillance technology
- The impact of citizen's human rights

Your answers will be used to compare countries and rank them from most to least strict when it comes to regulating surveillance, limiting the proliferation of surveillance technologies, and addressing injustices caused by surveillance towards state and non-state actors.

The questionnaire poses short questions to either be answered as Yes/No or on a scale of 1 to 10. No additional information or explanation for your answers is required at this time. Please feel free to be as honest and critical as possible so that we can reach an accurate classification.

Interview questions

Legislation:

- Does legislation in your country impact citizens' privacy and digital rights on the internet?

Yes / No / Maybe

- On a scale of 1 to 10 does the government have excessive control over existing privacy and freedom of speech laws?

With 1 being no control and 10 being complete control

- Does existing legislation in your country give state actors vague concessions under privacy and surveillance laws? Does/has the judiciary uphold such concessions?

Yes / No / Maybe

- Do national regulatory bodies that oversee surveillance technology in your country more broadly fail to operate in a free, fair, and independent manner?

Yes / No / Maybe

Surveillance technology:

- On a scale of 1 to 10, how proactive has your country's government been in acquiring new surveillance technologies?

With 1 being not proactive at all and 10 being extremely proactive

- On a scale of 1 to 10, how transparent has the state been in adopting new surveillance technologies in your country in the last five years?

With 1 being completely transparent and 10 being not transparent at all

- Has the state been transparent about the vendors it's been in touch with in acquiring surveillance tech for the country?

Yes / No / Maybe

Impact on citizen human rights:

- Does state surveillance of internet activities infringe on individuals' right to privacy?

Yes / No / Maybe

- On a scale of 1 to 10, to what extent has state surveillance impacted an individual's freedom of speech and dissent?

With 1 being no impact and 10 being extreme impact

- Are citizens subjected to extralegal intimidation or physical violence by state authorities? Rank each on a scale of 1 to 10; with 1 being not subjected at all and 10 being extremely subjected:

- *For the work that they do in their professions (journalists, human rights defenders, lawyers, politicians)*
- *For their identity and speech (religious minority, ethnic minority, gender and sexual minorities)*
- *Other*