

The Politics of Exposure: Audio Leaks and the Erosion of Privacy and Democracy in Pakistan

Faaiza Qazi¹

Published July 2025

I. INTRODUCTION.....	1
II. A HISTORY OF SURVEILLANCE.....	4
A. CONSTITUTIONAL RIGHTS.....	4
B. PREVIOUS JURISPRUDENCE.....	5
III. THE LEGAL AND REGULATORY FRAMEWORK.....	6
C. THE TELEGRAPH ACT, 1885.....	10
D. THE PREVENTION OF ELECTRONIC CRIMES ACT, 2016.....	10
IV. THE AUDIO LEAKS CASE.....	12
A. POLITICAL BACKGROUND.....	12
B. THE LITIGATION.....	15
1. Proceedings Before the Islamabad High Court.....	17
2. Supreme Court Intervention.....	25
V. CONCLUSION.....	26

I. Introduction

Information, or ‘data’, has always served as an indispensable form of capital, particularly for those in power. Its interception is equally woven into the fabric of history, finding use even in ancient Rome, where politician and orator Cicero spoke of the interception of his letters by the surveillance networks of major political players.² ‘How few are they who are able to carry a rather weighty letter without lightening it by reading,’ Cicero wrote to a friend.³

With the digital age, this once-elusive commodity has become instantly accessible, to be collected, analyzed or sold at will and whim, by a host of eager entities—ranging from hackers and malicious actors, to businesses, governments, and even terrorist organizations. This shift has been accelerated by the rapid, and rather uncritical, digitalization of core processes and activities by individuals, institutions and states, creating countless points of vulnerability across every level of society. From ordinary citizens to judges and politicians, no one is immune. And our phones, now living archives of our existence, have become one of the most easily exploited gateways into our inner worlds.

Data is therefore progressively, and unsurprisingly, wielded as a weapon: to influence, manipulate, and control. Its interception has evolved into an art form, with governments and private entities dedicating vast sums to develop increasingly invasive means of data collection. The misuse of data has thus become a defining feature of both global and domestic power struggles in the modern age. Surveillance technologies form a global industry, comprising hundreds of companies dedicated to developing these technologies, and selling them, indiscriminately, to government agencies across the world.⁴ Today, governments possess extensive surveillance frameworks—comprising internet service

¹ Faaiza is a practicing lawyer in Pakistan, currently on sabbatical as she pursues her LL.M. at Harvard Law School. She previously served as a judicial law clerk to a judge of the Supreme Court of Pakistan (January 2022 – January 2024) and holds an LL.B. from the University of London (International Programmes). Her areas of interest include constitutional law, legal theory, and public law, among others.

² Anthony Zurcher, *Roman Empire to the NSA: A World History of Government Spying*, BBC NEWS MAGAZINE (Nov. 1, 2023), <https://www.bbc.com/news/magazine-24749166>.

³ *Id.*

⁴ *The Global Surveillance Industry*, PRIVACY INT’L (Feb. 16, 2018), <https://privacyinternational.org/explainer/1632/global-surveillance-industry>

providers, telecommunication equipment vendors, and surveillance technologies—used to ‘lawfully’ intercept and collect data.⁵ The true extent to which data is intercepted outside, or under the guise of, the often overbroad laws and policies framed for the purpose, remains unknown.

This global rise in the use of surveillance technologies has raised alarms about the erosion of privacy and the weakening of democratic norms. The Pegasus Project, for instance, unveiled how governments—particularly authoritarian regimes—employ sophisticated spyware to infiltrate the devices of journalists, activists, and political adversaries, extracting sensitive information without consent.⁶ The Pegasus spyware can gather data, record video and audio, take screenshots and track location, all without the user’s knowledge. Infection can occur silently, without the target ever clicking on a link or answering a call. As of 2021, The Guardian reported that the technology had been sold to 40 governments around the world, ostensibly to combat terrorism and crime, though forensic analyses cast doubt on these justifications.⁷

This was the same year the Pegasus Project revealed India as one of several countries utilizing the spyware and released surveillance lists containing the identities of prominent persons that were targeted. The data collected was not disaggregated, and individual searches were therefore not attributable to specific countries; nor could it be said with certainty whether any particular hack was successful.⁸ Nevertheless, thousands of Indian citizens appeared on the surveillance list, including government ministers, opposition politicians, journalists and activists. The surveillance list also included hundreds of Pakistani phone numbers, including one belonging to former Prime Minister Imran Khan.⁹

Pakistan’s track record is no better. A 2013 report by Citizen Lab revealed the presence of command-and-control servers for FinFisher in Pakistan.¹⁰ FinFisher is a commercial network intrusion malware,¹¹ capable of intercepting communications, accessing private data, and recording audio and video from computers or mobile devices.¹² The server was employed on a network owned by the Pakistan Telecommunication Company Limited (PTCL),¹³ a now-privatized state-owned entity with 62% government shareholding.¹⁴

A 2015 report by Privacy International revealed that mass network surveillance has existed in Pakistan since *at least 2005*, with surveillance technologies obtained from both domestic and international companies, including Alcatel, Ericsson, Huawei, SS8 and Utimaco.¹⁵

The report also documented Pakistan’s consistent cooperation with the U.S. National Security Agency (NSA), exposing its participation in the NSA’s Fairview Program, and its

⁵ *Id.*

⁶ Paul Lewis, *Huge data leak shatters the lie that the innocent need not fear surveillance*, THE GUARDIAN (Jul. 18, 2021),

<https://www.theguardian.com/news/2021/jul/18/huge-data-leak-shatters-lie-innocent-need-not-fear-surveillance>.

⁷ Katharine Viner, *The Pegasus project: Why Investigations Like This Are at the Heart of The Guardian’s Mission*, THE GUARDIAN (Jul. 23, 2021),

<https://www.theguardian.com/news/2021/jul/23/pegasus-project-investigations-nso-spyware-mobile-phones>.

⁸ *Pegasus snooping: Pakistan probes whether PM Khan’s phone hacked*, AL JAZEERA (Jul. 20, 2021),

<https://www.aljazeera.com/news/2021/7/20/pegasus-snooping-pakistan-imran-khan-phone-hacked>.

⁹ Reuters, *PM Imran’s Number Among Those Targeted for Surveillance By India Using Israeli Spyware: Report*, DAWN (Jul. 19, 2021), <https://www.dawn.com/news/1636010>.

¹⁰ Morgan Marquis-Boire et al., *For Their Eyes Only: The Commercialization of Digital Spying*, The Citizen Lab (Apr. 30, 2013), <https://citizenlab.ca/2013/04/for-their-eyes-only-2/>.

¹¹ *Ownership explained*, DAWN (Mar. 05, 2025), <https://www.dawn.com/news/1895853>.

¹² *German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed*, AMNESTY INT’L (Sep. 25, 2020),

<https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/>.

¹³ Marquis-Boire et al., *supra* note 10.

¹⁴ *Ownership explained*, DAWN (Mar. 05, 2025), <https://www.dawn.com/news/1895853>.

¹⁵ *Tipping the scales: Security & surveillance in Pakistan*, PRIVACY INT’L (Jul. 2015),

https://www.privacyinternational.org/sites/default/files/2018-08/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf.

SKYNET initiative.¹⁶ Pakistan has featured strongly in the NSA's Fairview Program, which involves the mass surveillance of individuals within and outside the U.S., facilitated by a 'highly collaborative' partnership with AT&T, one of the largest telecommunications companies in the US.¹⁷ The SKYNET program, which algorithmizes terrorist detection by harvesting cellular metadata from Pakistani telecom service providers, was used to identify thousands of alleged 'extremists' in Pakistan between 2004 and 2016, who were later killed through drone strikes.¹⁸

In 2019, The Guardian reported that at least two dozen Pakistani government officials had been targeted using Israeli spyware, alongside lawyers, journalists, human rights activists, political dissidents, and diplomats.¹⁹ The malware reportedly exploited a vulnerability in WhatsApp, allowing operators to access encrypted messages and other sensitive data on the targets' devices.²⁰ While these attacks were not initially credited to Pakistani authorities, in 2023, an Israeli newspaper, Haaretz, reported that the FIA and various police units in Pakistan have been using the software since at least 2012.²¹ Local officials later confirmed that the spyware—a dated version of Israeli company Cellebrite's Universal Forensics Extraction Device (UFED)—had been acquired indirectly, through foreign agents, despite the lack of diplomatic ties between the countries.²²

Around the same time, it was revealed that Pakistan had acquired the services of a controversial Canada-based company, Sandvine, through a USD 18.5 million contract, to help build a nationwide 'web monitoring system'.²³ This system would use Deep Packet Inspection (DPI) to monitor communications, as well as measure and record traffic and call data, on behalf of the country's national telecommunications regulator, the Pakistan Telecommunication Authority (PTA).²⁴ This was seemingly pursuant to the Monitoring and Reconciliation of Telephony Traffic Regulations, 2010, issued by the PTA.²⁵ The PTA has alleged that it discontinued its use of DPI services in mid-2023.²⁶

In 2024, Pakistan tested a national internet 'firewall', reportedly using Chinese technology, which allowed the government to bolster its web monitoring capabilities, and regulate the use of popular platforms by blocking specific features within an app or a website.²⁷ According to Al Jazeera, this firewall was deployed at the country's main internet gateways, as well as the data centers of mobile service and major internet service providers, and triggered numerous complaints of poor internet connectivity.²⁸

¹⁶ *Id.*

¹⁷ Julia Angwin *et al.*, *AT&T Helped U.S. Spy on Internet on a Vast Scale*, THE NEW YORK TIMES (Aug. 15, 2015), <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html>.

¹⁸ Christian Grothoff & J.M. Porup, *The NSA's SKYNET program may be killing thousands of innocent people*, Ars Technica (Feb. 16, 2016), <https://arstechnica.com/information-technology/2016/02/the-nsas-sky-net-program-may-be-killing-thousands-of-innocent-people/>.

¹⁹ Stephanie Kirchgaessner, *Israeli spyware allegedly used to target Pakistani officials' phones*, THE GUARDIAN (Dec. 19, 2019), <https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones>.

²⁰ *Id.*

²¹ Oded Yaron, *Pakistan's Spy Agency Buys Israeli Cellphone Hacking Tech*, HAARETZ (Aug. 3, 2023), <https://www.haaretz.com/israel-news/security-aviation/2023-08-03/ty-article/.premium/pakistans-spy-agency-buys-israeli-cellphone-hacking-tech/00000189-b608-db5d-a5fd-b62979680000>.

²² Aamir Saeed, *Pakistani investigators using 'old version' of Israeli UFED digital intelligence software — officials*, Arab News (Aug. 07, 2023), <https://www.arabnews.com/node/2351011/pakistan>.

²³ Umer Ali and Ramsha Jahangir, *Pakistan moves to install nationwide 'web monitoring system'*, Coda (Oct. 24, 2019), <https://www.codastory.com/authoritarian-tech/pakistan-nationwide-web-monitoring/>.

²⁴ *Id.*

²⁵ *Id.*

²⁶ PPF Research Team, *PTA Clarifies Discontinuation of Internet Traffic Monitoring Services*, Pakistan Press Foundation (Oct. 28, 2024), <https://pakistanpressfoundation.org/pta-clarifies-discontinuation-of-internet-traffic-monitoring-services/>.

²⁷ Abid Hussain, *Pakistan tests secret China-like 'firewall' to tighten online surveillance*, AL JAZEERA (Nov. 26, 2024), <https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance>.

²⁸ *Id.*

The Lawful Intercept Management System (LIMS) is yet another surveillance mechanism employed by the Pakistani State, and can be used to retrieve the unencrypted data of any consumer, eavesdrop on their calls, and read text messages.²⁹ The surveillance tool recently came to light, following a series of leaked audios which resulted in litigation before the Islamabad High Court, and reveals a growing trend of politicized intrusion that now threatens the independence and integrity of key institutions, including that of the judiciary.

In a turbulent political and legal climate such as Pakistan's, the impact of leaked audios is immediate, driven by a widespread presumption of truth. They possess the power to coerce, damage reputations, and shape public narratives well before the facts come to light. By the time clarity emerges, public opinion has hardened, reputations have suffered, and the damage is done. The perpetrators remain elusive, while societal pressure descends upon the newest target.

To highlight the far-reaching consequences of such breaches of privacy, this article explores a selection of audio leaks that surfaced since 2022, implicating an array of influentials, including politicians and judges. By examining the legal, social, and political fallout of these audio leaks, this article seeks to establish how this strategically disseminated information functions not only as a tool of public embarrassment, but also as a means to exert pressure, undermine credibility, and influence institutional conduct and decision-making. It also outlines the glaring shortcomings in the domestic legal framework that enables such intrusions, offering no meaningful recourse, with an aim to highlight the evolving risks posed to democratic accountability and judicial independence in an age where state surveillance operates with little transparency, and even less restraint.

While this article is rooted in the Pakistani experience, its relevance transcends national borders. The tactics, technologies, and political incentives behind data weaponization are not unique to any one country—they reflect a global trend in which digital surveillance, audio manipulation, and leak-driven smear campaigns are increasingly deployed to shape public perception and suppress dissent. As democratic institutions around the world grapple with declining public trust, and as constitutional frameworks struggle to keep pace with technological advancement, the Pakistani example serves as a cautionary tale. It emphasizes the urgent need for international scrutiny, effective legal safeguards, and civic vigilance to protect the integrity of judicial systems, political discourse, and the private lives of citizens—before fundamental freedoms become (fundamentally) fiction.

The chapters to follow provide an overview of the constitutional and legal framework governing surveillance and privacy in Pakistan, while recounting previous instances where the Supreme Court of Pakistan has been faced with such issues. We thereafter delve into the audio leaks under consideration, going over the contents of the leaks, and the revelations made during the ensuing litigation.

II. A History of Surveillance

A. Constitutional Rights

Chapter II of the Constitution of the Islamic Republic of Pakistan, 1973 (“**Constitution**”) enunciates the fundamental rights of Pakistani citizens, with clause (1) of Article 8 rendering any law, custom or practice void to the extent that it is inconsistent with these rights. Clause (2) of Article 8 provides further protection to these fundamental rights, prohibiting the State from making any law which takes away or abridges them.

The most relevant, for the purposes of this article, are the following:

²⁹ Zaki Abbas, *The Surveillance System Keeping Tabs on Millions*, DAWN (Jul. 2, 2024), <https://www.dawn.com/news/1843299>.

Article 4 (Right of individuals to be dealt with in accordance with law, etc.) – This provides citizens with the inalienable right to ‘*enjoy the protection of law and to be treated in accordance with law*’, and prohibits any action ‘*detrimental to the life, liberty, body, reputation or property of any person*, except in accordance with law.

Article 9 (Security of person) – More commonly referred to as the ‘right to life’, it states that ‘*[n]o person shall be deprived of life or liberty save in accordance with law*’.

Article 14 (Inviolability of dignity of man, etc.) – More commonly referred to as the ‘right to privacy’, clause (1) of the Article states that ‘*[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable*’.

Article 19 (Freedom of speech, etc.) – This provides citizens the right to freedom of speech and expression, and protects the freedom of the press, albeit subject to ‘*reasonable restrictions imposed by law in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, commission of or incitement to an offence*.’ A right with many qualifiers.

Article 25 (Equality of citizens) – Clause (1) of this Article states that all citizens are equal before the law, and entitled to equal protection of the law.

B. Previous Jurisprudence

These fundamental rights have formed the basis for prior litigation regarding the legality of state surveillance before the superior courts of Pakistan. In the 1997 case of *Mohtarma Benazir Bhutto and others. v. President of Pakistan and others*, filed against the President’s order dissolving the National Assembly, the Supreme Court considered the legality of the Federal Government’s use of telephone tapping and eavesdropping.³⁰ One of the grounds raised by the President in the dissolution order was the violation of the right to privacy on a massive scale by Benazir Bhutto, then Prime Minister, and her Government. This included orders to the Intelligence Bureau (IB) under the Prime Minister’s supervision, to tap the phones of judges of the superior courts, leaders of political parties, and high-ranking military and civil officers. The Supreme Court, by a majority of 6-1, held that there was no basis in law for carrying out such surveillance. The tapping and eavesdropping of citizens of any class, group or status was violative of Articles 9 and 14 of the Constitution—with the former encompassing the right to be protected from encroachments on privacy and liberty, and the latter extending beyond the walls of any premises, to the individual, wherever they may be. Such actions constituted an offence under the 1885 Telegraph Act and could only be justified in cases of defense and national security.

In the case of *Justice Qazi Faez Isa and others v. The President of Pakistan*, the data of a Supreme Court judge, it was revealed, had been collected through covert surveillance of the Judge and his family in order to build up a case of asset concealment. The Honorable Justice Syed Mansoor Ali Shah, in his dissent, opined that privacy is a foundational requirement of democracy that guarantees “*the agency and autonomy of the individual and the right of every*

³⁰ The judgment is reported as **PLD 1998 SC 388**. While there is no official version of the judgment accessible online, a relatively decent copy thereof can be accessed at: <https://www.digitalrightsmonitor.pk/wp-content/uploads/2021/01/Mohtarma-Benazir-Bhutto-vs-the-President-of-Pakistan.pdf>.

person to have the freedom and liberty to live a life of dignity.”³¹ Privacy demands that all information about an individual is ‘*fundamentally his own, only for him to communicate or retain for himself.*’ He highlighted that the guarantee of privacy under Article 14 extends beyond the physical house, to the ‘*entire treasure of personal life of a human being,*’ and is deeply intertwined with the rights to life, personal liberty and dignity. The State could not intrude into this sanctum of personal space, other than for a larger public purpose. And the proper regulation of surveillance and interception was all the more important in ‘*fledgling democracies*’, where the rule of law had not firmly taken root. Any laxity in this respect could be ‘*a serious threat to constitutional guarantees of the people, in particular, and to democracy, in general.*’ The dissenting note emphasized the disastrous potential of unregulated surveillance, pushing nations into an ‘*abyss of totalitarianism,*’ and highlighted the need for adequate checks and balances.

III. The Legal and Regulatory Framework

Over the years, the Pakistani legislature has enacted several laws empowering state institutions—encompassing law enforcement agencies (LEAs), intelligence services, and regulatory bodies—to monitor and surveil citizens and their activities, including private communications and online activity. These legislative instruments authorize the collection, interception and retention of such data (“**lawful intercept(ion)**”), at times under broad grounds of national security and crime prevention. Some of these instruments include safeguards that would deter and punish individual and/or state misuse of these powers and technologies. However, in some cases, such safeguards are lacking, enabling those they empower to act arbitrarily, and with unbounded discretion.

This chapter examines the legal framework authorizing such surveillance, focusing on the operation of key statutes like the Pakistan Telecommunication (Reorganization) Act, 1996 (“**PTRA**”) and the Investigation for Fair Trial Act, 2013 (“**IFTA**”), as well as statutes such as the Telegraph Act, 1885 (“**Telegraph Act**”) and the Prevention of Electronic Crimes Act, 2016 (“**PECA**”). As we will see ahead, the PTRA falls in the latter category of instruments, conferring powers of interception in broad terms, without built-in safeguards.

Beyond the authorities established under the legislative instruments mentioned below, Pakistan also features a Federal Investigation Agency (FIA), established under the Federal Investigation Agency Act, 1974, and several intelligence agencies, such as the civilian-led Intelligence Bureau (IB), established in 1947; the subsequently established Inter-Services Intelligence Agency (ISI), Pakistan’s principal military intelligence agency; and the Military Intelligence (MI), among others. Through the subsequent chapters, we will see how the powers possessed by these authorities and agencies have been utilized in practice, and how they have responded to the privacy concerns raised by the audio leaks that form the subject matter of this article.

A. The Pakistan Telecommunication (Re-Organization) Act, 1996

The PTRA was passed for the regulation of the national telecommunications industry, and establishes the Pakistan Telecommunication Authority (PTA), a body comprising three-members, including a Chairman, appointed by the Federal Government.³² Apart from regulating telecommunication systems and licensees, along with several other functions, the PTA is tasked with ‘*promoting and protecting the interests of users of telecommunication services*’ in Pakistan, and performing ‘*such other functions as the Federal Government may, from time to time, assign to it.*’ There is nothing that expressly empowers, or obligates, the PTA to surveil or monitor citizens in Section 4, which lays out the ‘*Functions of the*

³¹ The judgment is reported as **PLD 2021 SC 1**. Justice Shah’s complete dissenting note can be accessed at: https://www.supremecourt.gov.pk/downloads_judgements/const.p.17.2020_dissenting_note_hj11.pdf. The judgment of the majority, comprising seven out of ten judges, can be accessed at: https://www.supremecourt.gov.pk/downloads_judgements/const.p.17.2019_detailed_reasoning.pdf.

³² Pakistan Telecommunication (Re-Organization) Act [PTRA], §3 (1996).

Authority’. Section 5 lays out the ‘*Powers of the Authority*,’ one of which is to ‘*collect information with respect to telecommunications within and outside Pakistan and review the impact thereof*.’ The PTA is also empowered to issue regulations for exercising its powers and for the performance of its functions. Under Section 57, the Federal Government is empowered to make rules, ‘*not inconsistent with [the] Act*’, for carrying out its purposes, including for ‘*enforcing national security measure[s] in telecommunication sector*’ and ‘*lawful interception*.’

Under Section 8 (1), the Federal Government is empowered to issue policy directives to the PTA, ‘*not inconsistent with the provisions of the Act*,’ on matters relating to *telecommunication policy*, as specified in clause (2), including requirements of national security. However, the subsequent clause (2A), inserted in 2006, states that ‘*[n]otwithstanding anything in sub-section (2)*,’ the Cabinet, or a committee authorized by it, is empowered to issue **binding ‘policy directive[s] on any matter related to telecommunication sector, not inconsistent with the provisions of [the] Act.’** Section 8 therefore vests the Federal Government with broad powers of control over the PTA. Section 2 (fa), states that the ‘Federal Government,’ for the purposes of the PTR, is the Ministry of Information Technology and Telecommunications (“**Ministry of IT&T**”).

Pursuant to Section 8, The Ministry of IT&T has previously issued the Mobile Cellular Policy, 2004—Clause 6.13 of which requires licensees to ‘*meet the requirements of authorized security agencies for legal interception of calls and messages*.’ Similarly, Clause 5.5.1 of the Telecommunication Policy, 2015, issued by the Ministry of IT&T, requires the PTA to develop an appropriate regulatory framework, in view of the requirements for lawful interception, cooperation with LEAs, and data retention obligations of operators, amongst others. Clause 9.9 provides that the Federal Government, through the Ministry of IT&T, will prescribe rules for lawful interception ‘*as mandated under [the PTR]*.’ PTA is obligated to devise a regulatory framework in light of these rules, in conjunction with the ‘*authorized agencies/organizations*’ of the Federal Government. This framework is to include mechanisms providing for the expansion of lawful intercept facilities. Notably, Clause 9.9.4 states that the functional model and systems employed for lawful interception are to be ‘*transparent and based on international standards*.’

Under Chapter VII of the PTR, titled *Miscellaneous*, we find Section 54, labeled **National Security**, which reads as follows:

“**54. National Security.**—(1) *Notwithstanding anything contained in any law for the time being in force, in the interest of national security or in the apprehension of any offence, the Federal Government may authorise any person or persons to intercept calls and messages or to trace calls through any telecommunication system.*

(2) *During a war or hostilities against Pakistan by any foreign power or internal aggression or for the defence or security of Pakistan, the Federal Government shall have preference and priority in telecommunication systems over any licensee.*

(3) *Upon proclamation of emergency by the President, the Federal Government may suspend or modify all or any order or licenses made or issued under this Act or cause suspension of operation, functions or services of any licensee for such time as it may deem necessary:*

Provided that the Federal Government may compensate any licensee whose facilities or services are affected by any action under this sub-section.”

Again, Section 54 vests the Federal Government with broad and disruptive powers of surveillance, particularly clause (1) which permits the Federal Government to authorize ‘*any person or person(s)*’ to surveil citizens by intercepting or tracing their communications.

The interplay of Sections 8 and 54 has been previously adjudicated upon by the Islamabad High Court (alternatively referred to as the “**IH Court**”). In the case of *CM Pak Limited v. Pakistan Telecommunication Authority*, CM Pak (Pvt.) Limited (better known by its trade name, Zong), along with customers of various telecom service providers had challenged the suspension of cellular services in Islamabad, on the ground of national security, pursuant to a policy directive issued by the Ministry of IT&T under Section 8 (2)(c) of the PTR. ³³ In this instance, the PTA had suspended cellular services on account of the annual *muhammad* processions, conducted by members of the *Shia* sect of Muslims. The IH Court had held that Section 8 (2)(c) was subservient to Section 54 (3) of the PTR, and, as such, the power to suspend cellular services on the ground of national security could only be utilized where there was a proclamation of emergency by the President. ³⁴ Any order of suspension on this ground in the absence of such a proclamation would be illegal and without lawful authority. ³⁵

This appears to be a sensible reading of the law, particularly given the repeated statement in Section 8 that policy directives are ‘*not [to be] inconsistent with the provisions of [the PTR]*’. A policy directive permitting suspension of cellular services in violation of Section 54 (3), which clearly establishes the parameters for such action, militates against this command.

However, the Supreme Court took a contrary view when the matter came before it, pursuant to an appeal filed by the Ministry of IT&T, holding that Sections 8 and 54 of the PTR had distinct purposes. ³⁶ The latter is ‘*reactive and defensive*’ in nature, coming into the field where a Proclamation of Emergency is issued by the President on account of grave circumstances, ‘*potentially involving a suspension of fundamental rights*’ under the Constitution. In such an instance the disruption in cellular services could be over an extensive area, for a prolonged period of time. The former, however, ‘*contemplates pre-emptive action*’, allowing for the disruption of services ‘*before any perceived threat in a specified area materializes*’. Such disruption of services was likely to be event specific and localized, for a shorter period of time. Thus, both provisions operate in ‘*separate spheres and situations with no conflict between them nor any primacy being given to one over the other*’. The policy directive had therefore been validly issued, and the only question before the Court was whether the PTA had exercised its power under the policy directive fairly, justly and for the advancement of the purposes of the Act, which the Court affirmed it had.

Using its powers to issue regulations, under Section 5 (2)(o), the PTA has also issued the Monitoring and Reconciliation of Telephony Traffic Regulations, 2010 which provide for the establishment and administration of monitoring systems by licensees. According to Regulation 2 the regulations are to apply to ‘*all Licensees and Access Providers*’, with the purpose being to monitor information passing through the processing equipment and accessories associated with these entities ‘*for verification of authorized use, reconciliation of total traffic terminated on the network of the Licensees to measure and record for billing verification, detect[ing] and controlling grey traffic, and determin[ing] the quality of licensed services*’. Regulation 4, read with Regulation 2 (n), mandates all Long-Distance and International (LDI) licensees and Access providers to establish a ‘*System*’, at their own cost, consisting of equipment ‘*deployed for the monitoring, aggregating, measuring and reconciling of traffic, monitoring and controlling of grey traffic, removal of asymmetry, billing and quality of the licensed service*’. Landline and infrastructure licensees are similarly required to establish a ‘*Monitoring System*’, under Regulation 4 (5), for monitoring telecommunication traffic, including both voice and data. Under clause (6) of Regulation 4, these systems must, at a minimum, be capable of monitoring, controlling, measuring and

³³ The judgment is reported as **PLD 2018 Islamabad 243**, and can be accessed at <https://mis.ihc.gov.pk/attachments/judgements/F.A.O.%2042-2016%20Against%20Order%20-finalFAONo.42of2016.CMPakLimitedv.ThePTA.etc.636552442049031490.pdf>.

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Ministry of Information Technology and Telecommunications and another v. C.M. Pak (Pvt.) Ltd. and another (PLD 2020 Supreme Court 551)*. The judgment can be accessed at https://www.supremecourt.gov.pk/downloads_judgements/c.a._977_2018.pdf.

recording traffic in real-time, and providing a complete list of Pakistani customers and their details, amongst other things.

On November 23, 2016, the PTA issued standard operating procedures (SOPs) on the Requisitioning of Call Data Recorded by Authorized Officers from telecommunication operators.³⁷ These SOPs require operators to share Call Data Records (CDRs) with designated officers from LEAs, provincial police departments, and the ISI and IB, in accordance with the specified procedures.

B. The Investigation for Fair Trial Act, 2013

The IFTA is the first law in Pakistan expressly purposed for the investigation and collection of evidence by means of modern techniques and devices, and to regulate the powers of law enforcement and intelligence agencies in this regard.³⁸ The preamble to the IFTA clearly evinces the legislative intent undergirding the Act: to ‘*prevent the law enforcement and intelligence agencies from using their powers arbitrarily*’ with respect to modern investigative techniques such as covert surveillance and human intelligence, property interference, wiretapping and communication interception.

In line with this intention, Section 27 of the IFTA establishes a Review Committee, comprising the Ministers of Defence, Interior and Law, which is mandated to meet every six months to determine whether warrants issued under the IFTA have been helpful in the prevention or prosecution of offences, or have contributed to achieving the object and purposes of the Act.

Under the IFTA, only the ‘applicants’—defined in Section 3(a) to mean the ISI, the ‘*three Services Intelligence Agencies*’, the IB and the Police—may apply to a High Court for a warrant of surveillance or interception. The applicants are required to notify an officer of appropriate rank to represent them for the purposes of the application (i.e. the ‘*authorized officer*’).

A warrant issued under the IFTA is to be used ‘*only and exclusively for preventing or lawfully investigating a scheduled offence or to collect evidence in respect thereof*’, with the application submitted for this purpose disclosing all previous warrants sought against the concerned individual.³⁹ The abuse of such a warrant to interfere or intervene in the privacy of any person is expressly prohibited.⁴⁰

Where there is reason to believe that any person is likely to be involved in, or has committed, any scheduled offence, a report is to be prepared in this regard, which includes supporting evidence.⁴¹ Before making any application before the Court, the applicant agency must seek the permission of the Interior Minister, by presenting the aforementioned report, along with supporting evidence.⁴²

As mentioned above, warrants of surveillance can only be issued in connection with the ‘*scheduled offences*’, which are listed in Schedule I to the IFTA. Schedule I lists only five laws and includes offences only ‘*to the extent of terrorist activities*’ covered therein. The execution of the warrant is to be undertaken by a ‘*Designated Agency or Body*’, which, per Section 3 (e), refers to any one or more agency or body, capable of implementing the warrant of interception, designated by the Federal Government through a notification. A warrant issued under the IFTA permits the interception and recording of the suspect’s telephonic communication, in addition to their video surveillance; interception, recording or

³⁷ ¶14, Preliminary Report submitted by CM Pak Limited (trade name, Zong) in Writ Petition No. 1805 of 2023 (*Mian Najam us Saqib v. Federation of Pakistan and others*). This is one of the petitions involved in the **Audio Leaks Case** and is discussed in further detail below. The Preliminary Report is available on file with the author.

³⁸ Investigation for Fair Trial Act [IFTA], Preamble (2013).

³⁹ *Id.* at §8(c).

⁴⁰ *Id.*

⁴¹ *Id.* at §5.

⁴² *Id.* at §§6-7.

procurement of their electronic communications; and interception and taking over of their communication equipment.

Service providers are indemnified and immunized against claims arising out of their grant of access to such information and are required to maintain confidentiality in the execution of the warrant, with penal consequences for staff members misusing such data.⁴³ They are also barred from extending their technical facilities of interception to any person or organization other than the Designated Agency or Body.⁴⁴

Section 15 of the IFTA permits the High Court to recommend departmental action against an officer applying for a warrant, if it finds that the application is based on insufficient or irrelevant considerations; or it has resulted in undue and inappropriate interference in the privacy of any person; or that the material and information collected or received demonstrates that the officer concerned did not apply himself fully while making the application. Under Section 29, the High Court is also competent to decide complaints from any person who claims the warrant is being misused, or that the applicant has acted in excess thereof.

Section 34 prohibits the misuse of intercepted material by ‘*any official of the applicant or of the Court or any other person associated with any function under [the IFTA]*’, whereas Section 35 criminalizes unauthorized surveillance or interception by ‘*[a]ny person who carries out any surveillance or interception*’, making these offences punishable with imprisonment up to five and three years, respectively, and/or a fine.

As one would expect in a democratic polity, the scope of lawful surveillance under the IFTA is fairly limited, encompassing only individuals involved in terrorist or anti-state activities. The Act does not permit, or envision, the mass-scale surveillance of citizens. Instead, it provides a framework for punishing such excesses. However, despite the strong evidence of active state surveillance in Pakistan, as discussed above, there is no record of any warrants having been sought or issued under the IFTA till date, nor are there any recorded instances of criminal liability being imposed under Sections 34 or 35 thereof.

C. The Telegraph Act, 1885

The Telegraph Act, 1885 (the “**Telegraph Act**”) regulates the use of apparatus and equipment related to wired and wireless telegraphs, telephones, teletype, and radio communications. Under Section 5, the Federal and Provincial Governments, or their authorized officers, are permitted to take possession of licensed telegraphs and to order the interception of messages on account of any public emergency, or in the interest of public safety. Under Section 5 (1)(b), the relevant Government may order the blocking, interception and/or disclosure of any message, or class of messages, to or from any person or class of persons, or relating to any particular subject, transmitted or received by any telegraph.

Section 7 empowers the Federal Government to make rules, ‘*consistent with [the] Act*’, for, amongst other things, ‘*the precautions to be taken for preventing the improper interception or disclosure of messages*’ and ‘*the period for which, and the conditions subject to which, telegrams and other documents belonging to, or being in the custody of, telegraph officers shall be preserved*’.

Under Section 25, any person intentionally damaging or tampering with telegraphs for the purpose of intercepting or acquainting themselves with the contents of any message, amongst other purposes, is punishable with up to three years of imprisonment and/or a fine. Under Section 26, officials misappropriating, blocking, altering, or unlawfully intercepting or disclosing messages, or divulging purport of telegraphic signals, are similarly liable to be imprisoned, for up to three years, and/or fined.

⁴³ *Id.* at §§18-19, 21.

⁴⁴ *Id.* at §17(2).

D. The Prevention of Electronic Crimes Act, 2016

The Prevention of Electronic Crimes Act, 2016 (“PECA”) was passed ostensibly to ‘*prevent unauthorized acts with respect to information systems*’ (i.e. cybercrime), and to establish corresponding offences and procedures. From its very inception, PECA has been the subject of great controversy, with the ambiguity and breadth of the original enactment, as well as the motives behind it, drawing criticism.⁴⁵ Subsequent amendments, often motivated by political expediency, have also been the subject of legal challenges, as they further intruded upon the freedom of speech guaranteed under Article 19 of the Constitution.⁴⁶

Under Section 3, PECA makes the unauthorized access of an information system, or data, a crime punishable with up to three months of imprisonment and/or a prescribed fine. The copying or transmission of such data is punishable with up to six months’ imprisonment and/or a prescribed fine, under Section 4. Section 19 makes the unauthorized interception of transmissions and data, with ‘*dishonest intention*’, an offence punishable with up to two years of imprisonment and/or a prescribed fine.

Previously, Section 29 permitted the Federal Government to establish, or designate a LEA as the investigation agency for the purposes of the Act, with the Federal Investigation Agency (FIA) having been designated agency. However, through the recent Prevention of Electronic Crimes (Amendment) Act, 2025, the Federal Government has now established a specialised body, the National Cyber Crime Investigation Agency (NCCIA), to inquire into, investigate, and prosecute the offences under the Act.

Section 32 obligates ‘*service providers*’ to retain specified traffic data for a minimum of one year, or such period as notified by the Authority,⁴⁷ and to provide that data to the investigation agency, or its authorized officer, where required, subject to the production of a warrant issued by the relevant court.

For the disclosure of content data, a warrant is to be sought by an authorized officer of the investigation agency, under Section 34, through an application before the relevant court demonstrating that ‘*there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence*’ under the Act. Such a warrant is valid for a period of seven days, though it may be extended with the Court’s approval.

Section 39 permits the real-time collection and recording of information, *where there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation*, pursuant to an order by the relevant court. If satisfied, the Court may direct an agency designated for this purpose under the IFTA. However, such an order is not to be for a period ‘*beyond what is absolutely necessary*’, and, ‘*in any event, for not more than seven days*’. The court may, however, extend this permission for a further specified period beyond seven days, on application.

⁴⁵ Farieha Aziz, *Project PECA I: How to silence a nation*, DAWN (Dec. 12, 2022), <https://www.dawn.com/news/1725805>.

⁴⁶ See, e.g., The Pakistan Electronic Crimes (Amendment) Ordinance, 2002 (News Release, *Pakistan: Repeal Amendment to Draconian Cyber Law*, HUMAN RIGHTS WATCH (Feb. 28, 2022), <https://www.hrw.org/news/2022/02/28/pakistan-repeal-amendment-draconian-cyber-law>); The Prevention of Electronic Crimes (Amendment) Act, 2025 (Kamran Adil, *2025 Amendments to The Prevention Of Electronic Crimes Act, 2016: An Introduction*, RESEARCH SOCIETY OF INT’L L. (Feb. 25, 2025), <https://rsilpak.org/2025/2025-amendments-to-the-prevention-of-electronic-crimes-act-2016-an-introduction/>).

⁴⁷ While this Authority was previously the Pakistan Telecommunication Authority (PTA), following the 2025 amendments to PECA, this role has been conferred on the newly established Digital Rights Protection Authority (DRPA), which is to oversee the regulation of social media platforms, and is empowered to enforce compliance through directives and penalties. The DRPA is yet to become functional. See *NA approves amendments to PECA law without opposition*, TRIBUNE (Jan. 23, 2025), <https://tribune.com.pk/story/2524015/na-approves-amendments-to-peca-law-without-opposition>.

The powers of the officer authorized by the investigation agency are provided under Section 35 and include the power to access or inspect specified information systems, obtain and copy *only* relevant data therefrom, and to require persons in possession of decryption information of an information system, device or data under investigation to grant access to the same in an unencrypted or decrypted form.

IV. The Audio Leaks Case

A. Political Background

The audio leaks in Pakistan must be seen in the context of the legal and political landscape in which they emerged. Former Prime Minister Imran Khan, founder and Chairman of Pakistan Tehreek-e-Insaf (PTI), came to power following the 2018 general elections, which were marred by allegations of military-facilitated rigging.⁴⁸ Once in power, Khan's government displayed increasingly authoritarian tendencies—including crackdowns on dissent by citizens, journalists, and opposition politicians, under the guise of anti-corruption, counterterrorism and sedition laws.⁴⁹ This erosion of democratic norms precipitated the formation of the Pakistan Democratic Movement (PDM) in 2020—an alliance of opposition parties including the Pakistan Muslim League-Nawaz (PML-N), Pakistan People's Party (PPP), Jamiat Ulema-e-Islam-Fazl (JUI-F), and others—united by a shared resolve to resist Khan's rule and challenge his apparent alignment with the military establishment.⁵⁰

By April 2022, Khan had been ousted through a no-confidence vote in the National Assembly: the first successful vote of its kind in Pakistan's history.⁵¹ Khan alleged foreign interference,⁵² and dissolved both the Punjab and Khyber Pakhtunkhwa provincial assemblies (where PTI held power),⁵³ in an attempt to pre-empt the general elections.⁵⁴

Following Khan's removal, Shehbaz Sharif—then Leader of the Opposition and head of the PML-N—was elected Prime Minister, and led the PDM coalition government.⁵⁵ He vowed to redress the economic and foreign policy failures of the Khan-led Government.⁵⁶ However, unofficially, the PDM was widely perceived to be working toward neutralizing the political momentum of Imran Khan and his political party, and limiting the influence of those viewed as sympathetic to them.⁵⁷

Following the PDM's coming into power, numerous cases were registered against former Prime Minister Khan,⁵⁸ with the charges ranging from corruption to irregularities in his marriage.⁵⁹ On May 9, 2023, protests erupted across Pakistan as Imran Khan was arrested

⁴⁸ *Pakistan election: Imran Khan claims victory amid rigging claims*, BBC (Jul. 26, 2018), <https://www.bbc.com/news/world-asia-44965868>.

⁴⁹ Asad Hashim, *HRW slams Pakistan over dissent crackdown, alleged rights abuses*, AL JAZEERA (Jan. 14, 2022), <https://www.aljazeera.com/news/2022/1/14/hrw-report-pakistan-dissent-crackdown-alleged-rights-abuses>.

⁵⁰ Shah Meer Baloch and Hannah Ellis-Petersen, *Pakistan's united opposition protests against Imran Khan's rule*, THE GUARDIAN (Oct. 17, 2020), <https://www.theguardian.com/world/2020/oct/16/pakistans-united-opposition-protests-against-imran-khans-rule>.

⁵¹ *Imran Khan ousted as Pakistan's PM after vote*, BBC (Apr. 10, 2022), <https://www.bbc.com/news/world-asia-61055210>.

⁵² *Id.*

⁵³ Umar Farooq, *Punjab, KP assemblies to dissolve on Dec 23: Imran*, DAWN (Dec. 17, 2022), <https://www.dawn.com/news/1726841>.

⁵⁴ Abid Hussain, *Another Khan party-led provincial assembly dissolved in Pakistan*, AL JAZEERA (Jan. 18, 2023), <https://www.aljazeera.com/news/2023/1/18/another-khan-party-led-provincial-assembly-dissolved-in-pakistan>.

⁵⁵ Q Zaman, *Shehbaz Sharif elected as Pakistan's new prime minister*, AL JAZEERA (Apr. 11, 2022), <https://www.aljazeera.com/news/2022/4/11/shehbaz-sharif-elected-as-pakistans-new-prime-minister-2>.

⁵⁶ Hussain, *supra* note 54.

⁵⁷ Imran Mukhtar, *PDM trying to pit PTI against army: Imran*, THE NATION (Mar. 21, 2023), <https://www.nation.com.pk/21-Mar-2023/pdm-trying-to-pit-pti-against-army-imran>.

⁵⁸ Abid Hussain, *Former Pakistani PM Imran Khan arrested at Islamabad court*, AL JAZEERA (May 9, 2023), <https://www.aljazeera.com/news/2023/5/9/former-pakistan-pm-imran-khan-arrested-outside-islamabad-court>.

⁵⁹ *Ex-PM Khan, wife arrested on new charges after acquittal in 'illegal' marriage case*, ARAB NEWS (Jul. 13, 2024), <https://www.arabnews.com/node/2548976/pakistan>.

from the premises of the Islamabad High Court based on corruption charges.⁶⁰ Thousands of protestors associated with PTI were arrested, of whom 105 were handed into military custody, and 85 were convicted by military courts.⁶¹

Not long after, on August 9, 2023, Pakistan's parliament was dissolved, statedly in order to prepare for a national election.⁶² The dissolution allowed the setting up of an interim government to oversee the next general elections, constitutionally mandated to be held within 90 days of the dissolution.⁶³ However, elections were not held until February 8, 2024, and were followed by widespread allegations of rigging, with yet another PDM-lateral coalition, led by the Pakistan People's Party (PPP) and Pakistan Muslim League-Nawaz (PML-N), forming the majority in parliament.⁶⁴ Soon after, Shehbaz Sharif, leader of the PML-N, was elected as Prime Minister,⁶⁵ while Asif Ali Zardari, leader of the PPP, was elected President.⁶⁶ This is the current government of Pakistan.

The primary focus of this article will be on a set of audio leaks that resulted in litigation before the Islamabad High Court ("**IH Court**") in what is commonly known as the '**Audio Leaks Case**'. This case laid bare the State's ability to undertake the mass surveillance of its citizens through the Lawful Intercept Management System (LIMS) and revealed the flaws in the domestic legal framework that enabled the misuse of such surveillance technologies. The revelations made during the Audio Leaks Case have reinforced longstanding suspicions of institutional manipulation and state complicity, heightening concerns over the integrity and independence of Pakistan's democratic institutions, including the judiciary.

The potential impact of such reputational warfare both on the individual and institutional level is evident from the aftermath of the numerous audio leaks surfacing in recent years, involving judges, politicians, and private individuals—many of whom are either directly affiliated with PTI or perceived to be aligned with Khan's political camp. For instance, Justice Mazahar Ali Akbar Naqvi faced great backlash following three leaked audios of veteran politician, Pervaiz Elahi, a then-senior Pakistan Muslim League-Quaid (PML-Q) leader, in which he featured as a central subject (the 'Elahi-Naqvi leaks').⁶⁷ The leaked audios, one of which was allegedly a call between Elahi and Justice Naqvi, surfaced on February 16, 2023, purportedly exposing attempts to ensure the fixation of one '*Muhammad Khan*' case, presumed to be the case of Elahi's former principal secretary Muhammad Khan Bhatti, before Justice Naqvi.⁶⁸ Bhatti had been implicated in a corruption case involving PKR 460 million (approximately USD 1.7 million at the time); this amount was allegedly procured as bribes from government officials to appoint them at posts of their choice.⁶⁹ Elahi attributed the audio leaks to a systematic campaign against the judiciary, run by the PDM coalition.⁷⁰

⁶⁰ Mukhtar, *supra* note 57.

⁶¹ *Special report: May 9, mayhem and military trials - a year on*, DAWN (May 9, 2024), <https://www.dawn.com/news/1832279>.

⁶² Abid Hussain, *Pakistan parliament dissolved to hold election without ex-PM Imran Khan*, AL JAZEERA (Aug. 9, 2023), <https://www.aljazeera.com/news/2023/8/9/pakistan-national-assembly-to-dissolve-for-polls-without-ex-pm-imran-khan>.

⁶³ Mukhtar, *supra* note 57.

⁶⁴ Abid Hussain, '*Mandate thieves*': *New Pakistan government takes shape amid slew of jabs*, AL JAZEERA (Feb. 14, 2024), <https://www.aljazeera.com/news/2024/2/14/mandate-thieves-new-pakistan-government-takes-shape-amid-slew-of-jabs>.

⁶⁵ Abid Hussain, *Shehbaz Sharif elected Pakistan PM for second term after controversial vote*, AL JAZEERA (Mar. 03, 2024), <https://www.aljazeera.com/news/2024/3/3/shehbaz-sharif-set-to-become-pakistans-new-pm-after-controversial-election>.

⁶⁶ *Asif Ali Zardari elected Pakistan's president for second time*, AL JAZEERA (Mar. 9, 2024),

<https://www.aljazeera.com/news/2024/3/9/asif-ali-zardari-elected-pakistans-president-for-second-time>.

⁶⁷ Imran Mukhtar, *Elahi in the spotlight as audio leaks involving top judge go viral*, THE NATION (Feb. 17, 2023), <https://www.nation.com.pk/17-Feb-2023/elahi-in-the-spotlight-as-audio-leaks-involving-top-judge-go-viral>.

⁶⁸ Iftikhar A. Khan, *FIA told to act against Parvez Elahi after 'audio leaks'*, DAWN (Feb. 17, 2023), <https://www.dawn.com/news/1737565>.

⁶⁹ *Asif Ali Zardari elected Pakistan's president for second time*, *supra* note 66.

⁷⁰ *Id.*

Not long after, on March 03, 2023, yet another audio leak implicating Justice Naqvi surfaced.⁷¹ This time the leaked audio allegedly featured PTI leader, Fawad Chaudhary, who could be heard instructing his brother, Faisal Hussain, a practicing lawyer, to inform Justice Naqvi of the ‘loaded truck’ that awaited him.⁷² The term was presumed to be a colloquial reference to a hefty bribe.⁷³

Following these leaks, Justice Naqvi became the subject of multiple complaints of misconduct before the Supreme Judicial Council (SJC) of Pakistan, a constitutional body tasked with monitoring and inquiring into the conduct, efficiency and capacity of superior court judges.⁷⁴ Faced with immense pressure, Justice Naqvi resigned as a judge of the Supreme Court on January 10, 2024,⁷⁵ deemed to be ‘retired’ with all the pensionary benefits granted to a judge of his rank,⁷⁶ with his resignation being accepted by the President the very next day.⁷⁷ However, on March 7, 2024, the SJC found Justice Naqvi guilty of misconduct and recommended his removal from the judicial office.⁷⁸ On March 20, 2024, President Zardari notified the removal of Justice Naqvi as a judge of the Supreme Court, based on the SJC’s recommendations, stripping him of his earlier status.⁷⁹ This made Justice Naqvi the first Supreme Court judge in Pakistan’s history to be declared guilty of misconduct, and removed.⁸⁰

Another controversial audio leak surfacing on April 23, 2023, brought then-Chief Justice of Pakistan (CJP), Umar Ata Bandial into the fold of affected judges. This leaked audio, the contents of which were rather benign, reportedly revealed a conversation between CJP Bandial’s mother-in-law, and PTI lawyer Khawaja Tariq Rahim’s wife, Mahjabeen Noon.⁸¹ The pair were heard discussing their concern for CJP Bandial, as he presided over a case regarding the delay in holding general elections (past the constitutionally mandated 90-day period mentioned above), and for their children’s safety, while expressing frustration with the incumbent Government.⁸²

Following these leaks, and numerous others, the Federal Government, on May 19, 2023, notified the formation of a three-member commission headed by then-Justice Qazi Faez Isa, to probe the recent audio leaks which raised concerns regarding the independence of the judiciary.⁸³ According to the Terms of Reference (TORs) framed for the Commission, it was to probe numerous leaked audios, including the Elahi-Naqvi leaks; the audio involving CJP

⁷¹ Staff Reporter, *New ‘leaked audio’ targets Fawad Chaudhry*, DAWN (Mar. 4, 2023), <https://www.dawn.com/news/1740310>.

⁷² Asif Ali Zardari elected Pakistan’s president for second time, *supra* note 66.

⁷³ Web Desk, *Do you know why truck means Rs.1 billion in Pakistan*, AAJ NEWS (Mar. 3, 2023), <https://english.aaaj.tv/news/30313930>.

⁷⁴ Web Desk, *‘Audio leaks’: Another reference filed against Justice Mazahar Naqvi in SJC*, GEO NEWS (Mar. 10, 2023), <https://www.geo.tv/latest/475497-audio-leaks-another-reference-filed-against-justice-naqvi-in-sjc>.

⁷⁵ Haseeb Bhatti, *Justice Sayyed Mazahar Ali Akbar Naqvi resigns as top court judge*, DAWN (Jan. 10, 2024), <https://www.dawn.com/news/1804705>.

⁷⁶ According to Clause 15 of the Supreme Court Judges Leave, Pension and Privileges Order, 1997, Judges are entitled to receive pensionary benefits upon resignation, provided they have served for the minimum number of years indicated therein. While no official version of the Order is available online, an unofficial version can be accessed at: <https://nasirlawsite.com/laws/scjlp.htm>.

⁷⁷ Abdullah Mohmand, *President Alvi accepts resignation of SC’s Justice Naqvi*, DAWN (Jan. 11, 2024), <https://www.dawn.com/news/1804928>.

⁷⁸ Terence J Sigamony, *SJC finds ex-SC judge Naqvi guilty of misconduct*, BUSINESS RECORDER (Mar. 8, 2024), <https://www.brecorder.com/news/40292594/sjc-finds-ex-sc-judge-naqvi-guilty-of-misconduct>.

⁷⁹ Staff Reporter, *President okays ex-judge Mazahar Naqvi’s dismissal for misconduct*, DAWN (Mar. 21, 2024), <https://www.dawn.com/news/1822816>.

⁸⁰ Sabih Ul Hussnain, *SJC Finds Justice (Retd) Mazhar Ali Akbar Naqvi Guilty Of Misconduct*, THE FRIDAY TIMES (Mar. 7, 2024), <https://thefridaytimes.com/07-Mar-2024/sjc-finds-justice-ret-d-mazhar-ali-akbar-naqvi-guilty-of-misconduct>.

⁸¹ Web Desk, *Audio call between CJP Bandial’s mother-in-law, PTI lawyer’s wife leaked*, THE NEWS INTERNATIONAL (Apr. 23, 2023), <https://www.thenews.com.pk/latest/1063519-audio-call-between-cjp-bandials-mother-in-law-pti-lawyers-wife-leaked>.

⁸² *President okays ex-judge Mazahar Naqvi’s dismissal for misconduct*, *supra* note 79.

⁸³ Nasir Iqbal, *Isa-led panel to probe veracity of audio leaks*, DAWN (May 21, 2023), <https://www.dawn.com/news/1754727>.

Bandial's mother-in-law; and audio leaks involving Najam us Saqib, the son of former CJP Saqib Nisar.⁸⁴ The lattermost of these leaks, involving Najam us Saqib, were also part of the Audio Leaks Case and will be explored in further detail below.

The Commission's TORs, as subsequently highlighted by former-PM Imran Khan, failed to account for the source of the leaks, and did not empower the commission to look into who was behind the unlawful and unconstitutional surveillance of those implicated.⁸⁵ It also triggered a power struggle within the nation's apex court, which undermined the already-waning public trust in the institution as a whole.

On May 22, 2023, this Inquiry Commission held its first and final hearing.⁸⁶ It ordered the publication of advertisements in local newspapers inviting those in possession of relevant information to provide the same to the Secretary of the Commission. The Attorney General for Pakistan (AGP) was directed to provide the Commission with transcripts of the recordings, and the details of a department/agency capable of forensically evaluating them, in the event that any of the individuals implicated disputed their veracity. The order noted that the Commission would meet again on May 27, 2023.

On May 26, 2023, a five-member bench of the Supreme Court, including CJP Bandial, took up several petitions against the May 19 notification, including those filed by then-SCBA President Zuberi, who was implicated in the Elahi-Naqvi leaks, and former-PM Khan.⁸⁷ The petitioners argued the notification constituted executive encroachment, as this inquiry fell in the Supreme Judicial Council's domain. The AGP, on the other hand, had requested that CJP Bandial recuse himself, given that an audio of his mother-in-law was also before the Inquiry Commission. CJP Bandial refused. The Court asserted that the permission of the CJP, a prerequisite for the formation of the commission, had not been sought. The matter was listed for May 30, 2023, until when the May 19 notification and the May 22 order would remain suspended. The case was not taken up again on May 30, and an official recusal application against CJP Bandial was moved by the Federal Government, which was dismissed on June 06, 2023.⁸⁸ The matter went into cold storage thereafter, and the suspension order remained in the field.

On April 30, 2025, a reconstituted five-member bench of the Supreme Court dismissed the petitions challenging the formation of the Inquiry Commission. It declared the matter had become infructuous, following the retirement of Justice Qazi Faez Isa, and the elevation of the other two members to the Supreme Court.⁸⁹ No further progress has been made in this case, and the perpetrators of the leaks continue to elude accountability. This is but one example of the devastating potential of such breaches of privacy, and their ability to influence institutional behavior and undermine integrity.

B. The Litigation

The primary audio leaks under consideration, relating to former premier Imran Khan, featured private conversations of prominent individuals, often surfacing at conspicuously strategic moments, triggered political controversy and legal battles. These audio leaks, invariably unauthenticated and of uncertain provenance, have unveiled political strategies and internal PTI communications, and alleged misconduct. While their contents drew widespread attention, for many the more significant concern was the *source* of these

⁸⁴ Audio call between CJP Bandial's mother-in-law, PTI lawyer's wife leaked, *supra* note 81.

⁸⁵ *Id.*

⁸⁶ Order of the Inquiry Commission dated May 22, 2023, <https://agfp.gov.pk/SiteImage/Misc/files/Commission%20Order.pdf>.

⁸⁷ Order of the Supreme Court dated May 26, 2023 in Constitution Petition Nos. 14 to 17 of 2023, https://www.supremecourt.gov.pk/downloads_judgements/const.p._14_2023.pdf.

⁸⁸ Order of the Supreme Court dated June 6, 2023, on the Civil Miscellaneous Application No. 3663 of 2023, filed in the *ibid* cases, seeking CJP Bandial's recusal.

https://www.supremecourt.gov.pk/downloads_judgements/const.p._14_2023_31052023.pdf.

⁸⁹ News Correspondent, *Pleas against audio leaks commission disposed of*, TRIBUNE (May 01, 2025), <https://tribune.com.pk/story/2543312/pleas-against-audio-leaks-commission-disposed-of>.

leaks—especially given how they abruptly surfaced, on both social and electronic media, attaining virality within mere hours. The original uploader(s) would be shrouded in the process, unidentifiable without proper skills or resources.

These audio leaks were eventually litigated before the Islamabad High Court (the ‘**IH Court**’), in what is often called the ‘**Audio Leaks Case**’. The first, the Bibi-Bukhari leak, involved the wife of former Prime Minister Imran Khan, Bushra Bibi—a key figure in numerous leaks surfacing online between 2022 and 2024, and one of the petitioners before the IH Court. On December 8, 2022, an audio of Bushra Bibi and former Special Assistant to Prime Minister Imran Khan, Zulfi Bukhari, surfaced wherein the former was heard asking Bukhari to sell watches that the deposed premier had acquired from the *Toshakhana* (i.e. the State repository of gifts), at his instructions.⁹⁰

This leak was linked directly to ongoing criminal proceedings against Khan and his wife for illegally retaining items from the *Toshakhana*, and was championed by members of the ruling coalition as proof of the pair’s guilt.⁹¹ Subsequent news reports document Bukhari stating that the leaked conversation took place on the Prime Minister’s safe line (i.e. a secure line from the Prime Minister’s House),⁹² though Bukhari had earlier deemed the audio clip fake, and demanded a forensic analysis.⁹³

The second leak, which surfaced online on April 29, 2023, contained clips of two conversations, referred to as the Najam-Chaddhar leak and the Najam-Aziz leak. Both of these clips featured Najam us Saqib—son of Saqib Nisar, the former Chief Justice of Pakistan (CJP)—who had been widely criticized during his tenure, including for his perceived alignment with PTI.⁹⁴ Together, these audio clips were taken to indicate that Najam had sought a bribe in exchange for securing a party seat (commonly referred to as a ‘ticket’) for PTI aspirant, Abuzar Chaddhar.⁹⁵

In the first part, Chaddhar is heard expressing his gratitude to Najam, with Najam emphasizing the former CJP’s immense efforts to secure Chaddhar’s ticket and urging Chaddhar to come visit his father at the office that day.⁹⁶ The second part reveals a conversation between Najam and Mian Uzair Aziz—one rich with profanity—where the two appear to be discussing the compensation owed to the former for helping secure Chaddhar’s ticket.⁹⁷

It is reported that Chaddhar was granted a PTI ticket in the party’s second phase of selections, when the former premier and Chairman of PTI, Imran Khan, reviewed and changed his earlier decision with respect to twenty-two party seats.⁹⁸

⁹⁰ News Correspondent, *New audio of Bushra, Zulfi emerges discussing ‘sale of watches’*, TRIBUNE (Dec. 8, 2022), <https://tribune.com.pk/story/2390083/new-audio-of-bushra-zulfi-emerges-discussing-sale-of-watches>.

⁹¹ Order of the Supreme Court dated June 6, 2023, on the Civil Miscellaneous Application No. 3663 of 2023, *supra* note 88.

⁹² Web Desk, *Zulfi Bukhari wonders no audio leak of Bushra Bibi calling him ‘son’ surfaces*, THE NATION (Jan. 9, 2023), <https://www.nation.com.pk/09-Jan-2023/zulfi-bukhari-wonders-no-audio-leak-of-bushra-bibi-calling-him-son-surfaces>.

⁹³ *Fresh audio surfaces, purportedly of Bushra Bibi discussing ‘sale of watches’ with Zulfi Bukhari*, DAWN (Dec. 8, 2022), <https://www.dawn.com/news/1725303/fresh-audio-surfaces-purportedly-of-bushra-bibi-discussing-sale-of-watches-with-zulfi-bukhari>.

⁹⁴ Web Desk, *Saqib Nisar didn’t work as CJP, but Imran Khan’s agent: PM Shehbaz*, ARY NEWS (May 7, 2023), <https://arynews.tv/saqib-nisar-didnt-work-as-cjp-but-imran-khans-agent-pm-shehbaz/>.

⁹⁵ Mansoor Malik, *Audio leak suggests ex-CJP’s son sought bribe from PTI aspirant*, DAWN (Apr. 30, 2023), <https://www.dawn.com/news/1750099>.

⁹⁶ Web Desk, *Audio leaks: PTI’s investigation does not find ex-CJP Saqib Nisar’s son guilty*, THE NATION (Apr. 30, 2023), <https://www.nation.com.pk/30-Apr-2023/audio-leaks-pti-s-investigation-does-not-find-ex-cjp-saqib-nisar-s-son-guilt>.

⁹⁷ *Saqib Nisar didn’t work as CJP, but Imran Khan’s agent: PM Shehbaz*, *supra* note 94.

⁹⁸ *Fresh audio surfaces, purportedly of Bushra Bibi discussing ‘sale of watches’ with Zulfi Bukhari*, *supra* note 93.

The former CJP had confirmed that the voice in the audio clips was his son's, though he stated the facts were doctored.⁹⁹ He admitted that he had recommended Chaddhar for the PTI ticket, which was both permissible and proper, but denied taking any bribe for this purpose.¹⁰⁰

PTI initiated its own investigation immediately after the audio leaks featuring Najam surfaced, though by the very next day, April 30, 2023, a representative of the party announced '*the allegation ha[d] been found false after investigation*'.¹⁰¹ It is unclear what this rather expeditious investigation entailed as none of the details have ever been made public.

Soon after, on May 02, 2023, the National Assembly passed a motion for the constitution of a Special Committee to probe into the audio leaks involving Najam us Saqib.¹⁰² This Committee was to conduct a forensic analysis of the audio, and interview the persons heard therein.¹⁰³ The same day, a ten-member Special Committee was constituted, and tasked with submitting a report on the leaks to the National Assembly, after a thorough investigation and inquiry.¹⁰⁴ The Committee was empowered to draw assistance from any investigative agency for this purpose.¹⁰⁵

Speaking to a private news channel, the Chairman of the Special Committee, Minister Muhammad Aslam Bhootani, stated that the Committee had called upon the Law and Interior Ministers, and the cyber wing of the Federal Investigation Agency, to ascertain the veracity of the audio clips.¹⁰⁶ The Committee was set to hold its first meeting on May 09, 2023, to set the terms of reference and summon the implicated individuals, including the former CJP.¹⁰⁷

On May 25, 2023, the Special Committee summoned Najam, Chaddhar and Aziz, to appear before it on its next hearing scheduled for June 01, 2023.¹⁰⁸ The Committee stated that the FIA had submitted its forensic report, which purportedly confirmed the voice as Najam's.¹⁰⁹

Around the same time, Najam was also summoned to appear before the judge-led Inquiry Commission on May 27, 2023, for the same leaked audios.¹¹⁰ However, the notification issued for forming the Inquiry Commission was suspended before the hearing could take place.¹¹¹

1. Proceedings Before the Islamabad High Court

On May 31, 2023,¹¹² Najam us Saqib challenged the legality of the Special Committee before the Islamabad High Court, and asked the Court to declare the recording, storing and use of private conversations of citizens to be violative of the fundamental rights protected under Articles 4, 9, 14, and 19 of the Constitution.¹¹³ He argued that the leaked audios were *fruit of*

⁹⁹ Sanaullah Khan, *Aslam Bhootani to lead 10-member NA panel probing alleged audio clip of ex-CJP's son*, DAWN (May 3, 2023), <https://www.dawn.com/news/1750674>.

¹⁰⁰ *Saqib Nisar didn't work as CJP, but Imran Khan's agent: PM Shehbaz*, *supra* note 94.

¹⁰¹ *Id.*

¹⁰² News Desk, '*PTI ticket deal*': NA demands probe into 'audio leak' of ex-CJP Nisar's son, TRIBUNE (May 2, 2023), <https://tribune.com.pk/story/2414704/pti-ticket-deal-na-demands-probe-into-audio-leak-of-ex-cjp-nisars-son>.

¹⁰³ *Saqib Nisar didn't work as CJP, but Imran Khan's agent: PM Shehbaz*, *supra* note 94.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ Malik Asad, *Panel summons ex-CJP's son over leaked audio*, DAWN (May 25, 2023), <https://www.dawn.com/news/1755618>.

¹⁰⁹ *Saqib Nisar didn't work as CJP, but Imran Khan's agent: PM Shehbaz*, *supra* note 94.

¹¹⁰ News Correspondent, *Leaks commission summons ex-CJP's son*, TRIBUNE (May 25, 2023), <https://tribune.com.pk/story/2418528/leaks-commission-summons-ex-cjps-son>.

¹¹¹ *SC suspends operation of govt notification on formation of judicial commission probing audio leaks*, DAWN (May 26, 2023), <https://www.dawn.com/news/1755908>.

¹¹² Based on the case details available for Writ Petition No. 1805 of 2023 (*Mian Najam us Saqib v. Federation of Pakistan etc.*) on the Islamabad High Court's website at <https://mis.ihc.gov.pk/frmCseSrch>.

¹¹³ Memo of Writ Petition No. 1805 of 2023, *Mian Najam us Saqib v. Federation of Pakistan etc.* (available on file with the author).

the poisonous tree—having been recorded through illegal surveillance—and were neither admissible as evidence, nor capable of being disseminated on news and media.¹¹⁴ He also asked the IH Court to suspend the summons issued to him by the Special Committee, and bar the Committee from conducting any further proceedings in the matter.¹¹⁵

The matter was placed before the Honorable Justice Babar Sattar on the very same day, with the Judge naturally questioning the source of the audios.¹¹⁶ The IH Court suspended the summons issued to Najam,¹¹⁷ and included the PTA, and the Ministries of Defence and Interior, amongst others, as respondents to the case.¹¹⁸ The respondents were directed to inform the Court of any existing legal framework for recording telephone conversations between citizens, while identifying the entities and agencies with the technological capability to record or surveil telecommunications, and the legal mechanism whereby they were permitted to do so.¹¹⁹ The Court also sought information on measures taken by the respondents to investigate and identify the parties responsible for the leaks.¹²⁰

Despite the suspension of the summons issued to Najam us Saqib, the Special Committee proceeded with its meeting scheduled for June 01, 2023, with the Chairman of the Committee proclaiming that no court could interfere in the proceedings of the Parliament.¹²¹ According to the press release issued for this meeting, the Committee summoned Najam, Chaddhar and Aziz once again, and sought the record of the financial transactions between them from the Ministry of Finance, in order to authenticate the alleged bribe.¹²² However, the Committee ceased to function soon after, when the National Assembly was dissolved on August 09, 2023,¹²³ statelily in preparation for general elections.¹²⁴

On September 12, 2023,¹²⁵ Bushra Bibi challenged the FIA's investigation into the Bibi-Bukhari leak before the Islamabad High Court, and requested a restraining order to prevent any adverse action against her.¹²⁶ Bibi similarly sought a declaration that the recording of private phones was illegal, and the leaked audios had no evidentiary value.¹²⁷ Due to the common plea taken in the petitions, this matter was also placed before Justice

¹¹⁴ SC suspends operation of govt notification on formation of judicial commission probing audio leaks, *supra* note 112.

¹¹⁵ *Id.*

¹¹⁶ Umer Mehtab, 'Who records the audios?' IHC judge seeks govt's response, DAWN (May 31, 2023).

https://www.dawn.com/news/1757045/who-records-the-audios-ihc-judge-seeks-govts-response?fbclid=IwY2xjawKsGJRleHRuA2FlbQlXMAbicmlkETE0Wk1WSIM0UHpZMGhqMXZ0AR5G6HMDBlzSwtWpy52PV95zaWACeXUH_KnhGuR32l04IMBR2a0hdJ4-S2TEw_aem_muwjYp725R9_rJC6qxQzDg.

¹¹⁷ SC suspends operation of govt notification on formation of judicial commission probing audio leaks, *supra* note 112.

¹¹⁸ Terence J Sigamony, *Probe into alleged audio leaks: IHC suspends summons issued to ex-CJP's son by NA panel*, BUSINESS RECORDER (Jun. 1, 2023), <https://www.brecorder.com/news/40245373>.

¹¹⁹ Mehtab, *supra* note 117.

¹²⁰ *Id.*

¹²¹ News Correspondent, *Parliamentary body on audio leaks meets today*, THE NEWS (Jun. 1, 2023),

<https://www.thenews.com.pk/print/1075808-parliamentary-body-on-audio-leaks-meets-today>.

¹²² Press Release, *NA Special Committee on Audio Leaks was held today*, National Assembly of Pakistan (Jun. 1, 2023), https://na.gov.pk/en/pressrelease_detail.php?id=5610.

¹²³ Hasnaat Malik, *Govt challenges IHC's leak case order*, TRIBUNE (Jul. 6, 2024).

<https://tribune.com.pk/story/2477102/govt-challenges-ihcs-leaks-case-order>.

¹²⁴ Abid Hussain, *Pakistan's National Assembly likely to be dissolved on August 9*, AL JAZEERA (Aug. 4, 2023),

<https://tribune.com.pk/story/2477102/govt-challenges-ihcs-leaks-case-order>.

¹²⁵ Based on the case details available for Writ Petition No. 2758 of 2023 (*Bushra Imran v. Federation of Pakistan etc.*) on the Islamabad High Court's website at <https://mis.ihc.gov.pk/frmCseSrch>.

¹²⁶ Shehzad Ali, *Zulfi Bukhari audio leak: Bushra Bibi moves IHC against harassment by police*, FIA, SAMAA (Sep. 11, 2023),

<https://www.samaa.tv/20873434-zulfi-bukhari-audio-leak-bushra-bibi-moves-ihc-against-harassment-by-police-fia>.

¹²⁷ Hussain, *supra* note 125.

Sattar, who directed the FIA to act in accordance with law,¹²⁸ and ordered that Bibi and Najam’s cases be heard together.¹²⁹

Despite this, the FIA issued a summons to Bibi for ‘voice-matching’ her audio on September 19, 2023 (i.e. through a forensic voice comparison),¹³⁰ which Bibi challenged through separate proceedings before the IHC.¹³¹ On September 22, 2023, Justice Sattar suspended the summons and sought a response from the FIA regarding the allegations made by Bibi.¹³²

Throughout the course of these clubbed cases, the Federal Government, including its various divisions and departments, as well as the LEAs and intelligence agencies before the IH Court, consistently denied that any agency or body possessed the technological capacity or authorization to conduct surveillance under the laws of Pakistan.¹³³ The ISI had asserted that it lacked the capacity to even ascertain the source of the leaks released on social media platforms,¹³⁴ with the FIA adding that it had requested this information from the relevant platforms.¹³⁵ The IB stated that it could neither confirm, nor deny the tapping of phones,¹³⁶ though it was willing to make a detailed presentation in the Judge’s chambers, as the issue involved ‘*sensitivities and security concerns*’ that could not be addressed in open court.¹³⁷ The Prime Minister’s Office had pleaded ignorance, claiming that it maintains an arms-length relationship with intelligence agencies, and does not interfere with their operational details and working, as doing so would be against the interest of national security.¹³⁸

While the respondents attempted to attribute the leaks to unidentified ‘*hostile agencies*’, the IH Court rejected this notion, finding it difficult to countenance that leaks related to the highest public offices of the country could be the ‘*[handiwork] of hostile agencies or elements [operating] beyond the remit of the state of Pakistan and without its knowledge.*’¹³⁹

As the national regulator for telecommunications, the Pakistan Telecommunication Authority (PTA) played a central role in these proceedings, with its Chairman being summoned in person by the IH Court to clarify contradictions and ambiguities in the Authority’s

¹²⁸ Naeem Asghar, *IHC suspends FIA summons notice to Bushra Bibi*, TRIBUNE (Sep. 23, 2023), <https://tribune.com.pk/story/2437368/ihc-suspends-fia-summons-notice-to-bushra-bibi>.

¹²⁹ Malik Asad, *IHC clubs petitions of Bushra, ex-CJP’s son in audio leak case*, DAWN (Sep. 13, 2023), <https://www.dawn.com/news/1775580>.

¹³⁰ Ali, *supra* note 127.

¹³¹ *IHC suspends FIA call-up notice to Bushra Bibi*, THE NEWS (Sep. 23, 2023), <https://www.thenews.com.pk/print/1112463-ihc-suspends-fia-call-up-notice-to-bushra-bibi>.

¹³² Ali, *supra* note 127.

¹³³ These statements were made at various points in the course of the proceedings. *See, e.g.*, ¶3 of Order dated October 30, 2023, passed in W.P. Nos. 1805/2023 and 2578/2023 (collectively, the “**clubbed cases**”), where the Secretary to the Prime Minister, and the Secretaries for the Ministries of Defence and Interior denied the grant of permission to any agency to intercept or record the phone calls of citizens, available at https://mis.ihc.gov.pk/attachments/judgements/162135/3/Writ_Petition_No._1805_of_2023_correct_638344257731240577.pdf. A similar statement by the Attorney General for Pakistan, on behalf of the Federal Government, and with respect to the FIA and ISI is recorded in ¶¶1-3 and ¶9 of Order dated December 20, 2023, *supra* note 133. ¶3 of Order dated March 4, 2024, *infra* note 136, records PTA’s statement that it had no authority to permit any entity to intercept telecommunications or data and had not authorized any telecom operator to do so.

¹³⁴ Order dated December 20, 2023, at ¶2 (passed in the clubbed cases).

https://mis.ihc.gov.pk/attachments/judgements/162135/3/W.P._No._1805-2023_638388407670901804.pdf.

¹³⁵ *Id.* at ¶1.

¹³⁶ This statement was made by the Director General IB, Fawad Asadullah, in open court. Though it was not recorded in the order from that date (i.e. the IHC Order dated March 4, 2024, *infra*), it was mentioned by several court reporters/journalists. Fiaz Mahmood, *IB neither confirms, nor denies audio tapping*, TRIBUNE (Mar. 5, 2024), <https://tribune.com.pk/story/2458416/ib-neither-confirms-nor-denies-audio-tapping>.

¹³⁷ Order dated March 4, 2024, passed in the clubbed cases, https://mis.ihc.gov.pk/attachments/judgements/162135/3/Writ_Petition_No.1805_of_2023_638457498664982370.pdf.

¹³⁸ Malik Asad, *PMO doesn’t interfere in spy agencies work, IHC told*, DAWN (Nov. 7, 2023), <https://www.dawn.com/news/1787141>. This statement was made through written submissions (available on file with the author), and is mentioned in the Court’s June 25 Order, *infra* note 184.

¹³⁹ Paragraph 5 of Order dated October 30, 2023, passed in the clubbed cases, https://mis.ihc.gov.pk/attachments/judgements/162135/3/Writ_Petition_No._1805_of_2023_correct_638344257731240577.pdf.

statements.¹⁴⁰ The PTA had denied any authorization or direction to intercept information,¹⁴¹ but had failed to provide an adequate response when questioned about the regulatory framework for lawful interception.¹⁴² This was despite the Court pointing out that telecom service providers (TSPs) are mandated to facilitate lawful interception under their license terms.¹⁴³ In subsequent hearings, the PTA submitted that TSPs were required to maintain the LIMS infrastructure due to the legal requirements under Section 54 of the Pakistan Telecommunication (Re-Organization) Act, 1996 (PTRA).¹⁴⁴ While conceding that the requirement to maintain such infrastructure was being enforced, the PTA claimed that, in the absence of instructions from the Federal Government, the framework and infrastructure for lawful interception lay idle.¹⁴⁵ It denied facilitating or permitting any agency or entity to use the LIMS infrastructure to surveil citizens, and claimed to be unaware of any such activity.¹⁴⁶ The Chairman of the PTA instead asserted that 90% of phones were already infected with a virus, which allowed their cameras to be operated,¹⁴⁷ and referred to the widely used Pegasus spyware, which could infiltrate phones within a minute.¹⁴⁸

Noting that the PTA had not been forthcoming, the IHC subsequently impleaded all the mobile service providers licensed to operate in Pakistan, and the six largest fixed-line service providers.¹⁴⁹ These service providers were directed to apprise the Court of the license provisions pertaining to lawful interception, while explaining how such requirements work in practice, and to disclose all communications with the PTA, or any LEA or intelligence agency, in this regard.¹⁵⁰ The impleaded mobile service providers included Pakistan Mobile Communications Limited (using trade name, Jazz), Pak Telecom Mobile Limited (using trade name, Ufone) Telenor Pakistan (Private) Limited (Telenor) and China Mobile Pakistan Limited (using trade name, Zong).¹⁵¹ As of March 2025, these companies hold market shares of 37.33%, 13.58%, 21.88%, and 26.23%, respectively—making up 99.02% of the cellular market—with over 195 million subscribers collectively.¹⁵² The remaining 0.98% of the market, with over 1.9 million subscribers, belongs to the military-run Special Communications Organization (SCO),¹⁵³ which holds an effective monopoly in the Gilgit-Baltistan, and Azad Jammu and Kashmir regions of Pakistan.¹⁵⁴

The proceedings took an interesting turn when, on March 25, 2024, Justice Sattar and five other judges of the Islamabad High Court wrote a groundbreaking letter to the Supreme Judicial Council (SJC).¹⁵⁵ The Supreme Judicial Council, a constitutional body, led by the

¹⁴⁰ See Paragraph 1 (Main Case) of Order dated March 4, 2024, *supra* note 136; Malik Asad, *PTA head summoned to clarify position on audio leak*, Dawn (Mar. 5, 2024), <https://www.dawn.com/news/1819257>.

¹⁴¹ Recorded by the Court at paragraph 3 of Order dated March 4, 2024, *supra* note 136. The actual statement was made in the report dated October 30, 2023, submitted to the Court by PTA (available on file with the author).

¹⁴² See Paragraph 3 of Order dated December 20, 2023, *supra* note 133.

¹⁴³ *Id.*

¹⁴⁴ Paragraph 1 of Order dated March 14, 2024, passed in the clubbed cases, available at https://mis.ihc.gov.pk/attachments/judgements/162135/3/W.P._No._2758-2023_638464493578676281.pdf.

¹⁴⁵ *Id.*

¹⁴⁶ Paragraph 2 of Order dated March 14, 2024, *supra* note 143.

¹⁴⁷ Again, this is a statement made by the Chairman, PTA in open court, though it was not noted in the Order from that date (i.e. Order dated March 14, 2024, passed in the clubbed cases). News Correspondent, *PTA denies role in Bushra Bibi's 'audio leak'*, TRIBUNE (Mar. 15, 2024), <https://tribune.com.pk/story/2459376/pta-denies-role-in-bushra-bibis-audio-leak>; Malik Asad, *Phone hacking has become too easy, PTA chief tells IHC*, DAWN (Mar. 15, 2024), <https://www.dawn.com/news/1821570>.

¹⁴⁸ Paragraph 2, Order dated March 14, 2024, *supra* note 143.

¹⁴⁹ Paragraph 4, Order dated December 20, 2023, *supra* note 133.

¹⁵⁰ *PTA denies role in Bushra Bibi's 'audio leak'*, *supra* note 148.

¹⁵¹ While the amended memo of the parties (i.e. which reflects the parties impleaded by the Court) is unavailable, these are the telecom service providers that made submissions before the Court.

¹⁵² Based on the Cellular Market Share (<https://www.pta.gov.pk/category/telecom-indicators/166>) and Monthly Mobile Cellular Subscribers (<https://www.pta.gov.pk/category/telecom-indicators/164>) recorded by the Pakistan Telecommunication Authority as of June 2025.

¹⁵³ *PTA denies role in Bushra Bibi's 'audio leak'*, *supra* note 148.

¹⁵⁴ Farman Ali, *Army's telecom wing allowed 3G, 4G services trial run in GB*, DAWN (Apr. 26, 2018), <https://www.dawn.com/news/1403965>.

¹⁵⁵ PTI, *Six Pak high court judges allege intelligence agencies' interference in judicial matters*, DECCAN HERALD (Mar. 27, 2024).

Chief Justice of Pakistan, and comprising other members of the superior judiciary, is responsible for inquiring into the capacity, efficiency and conduct of superior court judges.¹⁵⁶ In the absence of any settled protocol, the judges sought guidance with regard to their duty to report and respond to actions by members of the executive, including operatives of intelligence agencies, intended to interfere with the discharge of judicial duties and intimidate members of the judiciary, including members of the courts that the High Court supervises.¹⁵⁷ This is referred to as the ‘**Six Judges’ Letter**.’

Soon after, on March 27, 2024, multiple applications were filed seeking the recusal of Justice Sattar from the clubbed cases.¹⁵⁸ The applicants included the Pakistan Telecommunication Authority (PTA), Federal Investigation Agency (FIA), Intelligence Bureau (IB), and the Pakistan Electronic Media Regulation Authority (PEMRA), which had earlier been impleaded by the IH Court (collectively, the “**applicants**”).¹⁵⁹ The common ground in these applications was that Justice Sattar was a signatory to the Six Judges’ Letter, wherein serious allegations had been levelled against operatives of agencies, especially the military-run Inter-Services Intelligence (ISI).¹⁶⁰ Several other grounds were raised to justify the requests for recusal, including an earlier refuted ground that Justice Sattar had represented the PTA and various telecom service providers, prior to his elevation as a judge of the IH Court.¹⁶¹

The April 29 Order (2024)¹⁶²

The IH Court heard arguments with respect to these recusal applications on April 29, 2024, and questioned what the Six Judges’ Letter, which referenced intelligence agencies, naming only the ISI, had to do with the applicant agencies, which were independent bodies. None of the applicants could provide a response. Justice Sattar asked whether the applicants were involved in any of the incidents cited in the Six Judges’ Letter; the applicant agencies responded they were not. Thus, despite ample opportunity, the applicants failed to substantiate how the Six Judges’ Letter had any bearing on them.¹⁶³

In his subsequent forty-page order, passed with respect to the recusal applications, Justice Sattar cited a litany of superior court decisions on the recognized grounds for seeking the recusal of a judge, while emphasizing how the grounds raised by the applicants failed to meet the threshold set therein.¹⁶⁴ The Judge highlighted how the use of recusal requests to scandalize the court and intimidate judges had been deprecated by the superior courts.¹⁶⁵ Based on the cited jurisprudence, the IH Court found that the applications were *mala fide* (i.e. in bad faith) and frivolous, forming part of a collusive scheme to intimidate the Presiding Judge into recusing himself, without any legitimate cause.¹⁶⁶ The High Court highlighted the lackluster assistance provided to the Court by the Federal Government and its agencies and instrumentalities, as well as the refusal to engage with the subject matter in a candid manner, despite the serious allegations of State complicity in the breach of citizens’ fundamental rights to life, privacy and dignity.¹⁶⁷ This indicated a lack of desire to protect the fundamental rights of citizens.¹⁶⁸ The applications were consequently dismissed, with heavy fines imposed

<https://www.deccanherald.com/world/six-pak-high-court-judges-allege-intelligence-agencies-interference-in-judicial-matters-2954496>.

¹⁵⁶ The SJC is established under Article 209 of the Constitution.

¹⁵⁷ *PTA denies role in Bushra Bibi’s ‘audio leak’*, *supra* note 148.

¹⁵⁸ These dates are based on the office stamps on the actual applications filed before the Court (available on file with the author).

¹⁵⁹ Order dated April 29, 2024, at 1, passed in the clubbed cases (available on file with the author).

¹⁶⁰ *Id.* at 2.

¹⁶¹ *Id.*

¹⁶² *Id.*

¹⁶³ *Id.* at 1-9.

¹⁶⁴ *Id.* at 10-58 (laying out, in great detail, the jurisprudence relevant to the recusal of judges).

¹⁶⁵ *Id.* at 54.

¹⁶⁶ *Id.* at 59.

¹⁶⁷ *Id.* at 10-58

¹⁶⁸ *Id.*

on each applicant, to be paid personally by the public official within each applicant-authority who authorized the application.¹⁶⁹

The May 29 Order (2024)¹⁷⁰

In the subsequent hearing, on May 29, 2024, the Federal Government was asked whether the provisions of the Investigation for Fair Trial Act, 2013 (IFTA) had been given effect, and whether any warrants had been solicited from the High Courts, through the procedure provided in the Act.¹⁷¹ The IH Court also asked whether the Review Committee provided under Section 27 of the IFTA had been established.¹⁷² The Federal Government sought time to respond to these queries. The Federal Government also admitted that no criminal case had been registered under Section 19 of the Prevention of Electronic Crimes Act, 2016 (PECA), which criminalizes unauthorized interceptions, and asserted that the would-be complainants (i.e. Bushra Bibi and Najam us Saqib) had not assisted the relevant investigation agencies.¹⁷³ When the IH Court asked whether the registration of a criminal case was contingent on a complainant appearing before the relevant authority, even where the commission of an offence was in the knowledge of the State, the Federal Government answered in the negative.¹⁷⁴

The IH Court confronted the respondents with several news reports referencing reports the ISI and IB had filed with the Supreme Court in May 2015, wherein the agencies admitted to tapping the telephones of thousands of citizens.¹⁷⁵ These reports had been filed in a decades-old *suo motu* case taken up by former Chief Justice of Pakistan, Sajjad Ali Shah, in 1996, when he found a recording device attached to his telephone, ostensibly by certain spy agencies.¹⁷⁶ When asked whether the reported phone tapping was undertaken in compliance with the IFTA, which was in force at the time, the Federal Government again sought time to respond.¹⁷⁷

Based on the repeated denials of any State-authorized surveillance, the IH Court passed an order (the “**May 29 Order**”) restraining intelligence and law enforcement agencies from surveilling any citizens, except in accordance with a warrant duly issued under the IFTA.¹⁷⁸ Moreover, it restrained the PTA and telecom service providers from authorizing the use of their equipment for purposes of any surveillance, or interception of phone calls or data.¹⁷⁹ The Federal Government was also directed to disclose all requests made for warrants under the IFTA, and details of any surveillance conducted under the Telegraph Act or the PTFA, since the enactment of the IFTA.¹⁸⁰ Similar directions were issued to the Ministries of Defence, Interior and Law, with a further direction to apprise the Court of the manner in which they have discharged the obligations of the Review Committee, under Section 27 of the IFTA.¹⁸¹ Lastly, the PTA was directed to disclose any standard operating procedures (SOPs) or instructions issued to telecom operators to facilitate lawful interception and/or share telecom data with anyone in breach of provisions of the IFTA, while substantiating their legal authority.¹⁸²

¹⁶⁹ *Id.* at 54.

¹⁷⁰ IHC Order dated May 29, 2024, passed in the clubbed cases, available at https://mis.ihc.gov.pk/attachments/judgements/162135/3/W.P._No._2758-2023_638526798046378547.pdf.

¹⁷¹ *Id.* at 7.

¹⁷² *Id.*

¹⁷³ *Id.* at 8.

¹⁷⁴ *Id.* at 7.

¹⁷⁵ *Id.* at 9.

¹⁷⁶ Nasir Iqbal, *JIT wiretap controversy reignites old debate*, DAWN (Jun. 26, 2017), <https://www.dawn.com/news/1341756>.

¹⁷⁷ Order dated May 29, 2024, *supra* note 171, at 8.

¹⁷⁸ *Id.* at 11.

¹⁷⁹ Iqbal, *supra* note 177.

¹⁸⁰ Order dated May 29, 2024, *supra* note 171, at 12.

¹⁸¹ *Id.* at 11.

¹⁸² *Id.* at 14.

The June 25 Order (2024)¹⁸³

These Standard Operating Procedures, issued by the Ministry of Interior, were provided to the IH Court on the next date of hearing, June 25, 2024, and laid out the procedure for telecom service providers to share messages, call data records (CDRs), live locations and related consumer data (collectively, “**consumer data**”).¹⁸⁴ The Court questioned the authority of the Ministry of Interior to issue directions to the PTA, and refuted attempts to justify this on the basis of Section 8 of the Pakistan Telecommunication (Re-Organization) Act, 1996 (PTRA), which enables the Federal Government to issue policy directions to the PTA.¹⁸⁵ When asked whether any rules had been framed by the Federal Government for regulating the manner of issuing authorizations and conducting surveillance under Section 54 of the PTRA, the Federal Government was unable to answer, and instead attempted to argue that the matter should be heard in the Judge’s chambers, due to its implications for national security.¹⁸⁶ The IH Court rejected this request, yet again, emphasizing the importance of open court proceedings.¹⁸⁷ National security could not be equated with the security of an ‘*inanimate monolith*’, the Court commented.¹⁸⁸ It is the collective security of citizens to be protected by the State. The leaked conversations had no bearing on national security and did not warrant in-chamber proceedings. It was deemed inconceivable—in a nation governed by the rule of law—that public functionaries may be permitted to act pursuant to secret policies, with no legal backing, especially when such policies have a bearing on the fundamental rights of citizens.¹⁸⁹

It was also revealed, based on the reports submitted by the Federal Government and the intelligence and law enforcement agencies, that not a single warrant had been issued under the IFTA, since its enactment.¹⁹⁰

The Inspector General of the local Islamabad Capital Territory Police (“**ICT Police**”) also appeared on this date and submitted that the ICT Police had never sought a warrant for surveillance under the IFTA, though consumer data had been sought from telecom service providers (TSPs) for the investigation of criminal matters, pursuant to the relevant criminal laws. Once a criminal complaint was lodged, the police authorities had sufficient powers under criminal law to procure such data, and did not need to resort to seeking permission under the Telegraph Act, PTRA or IFTA. It was added that TSPs had ceased their sharing of such data with the ICT Police following the Court’s last order, which was hindering investigation in various cases.¹⁹¹

Most crucially, it was on this date of the hearing—June 25, 2024—that the TSPs provided a detailed account of their license requirements and the LIMS. The TSPs disclaimed liability by asserting that they were under a legal obligation to comply with the lawful intercept regime prescribed by the PTA, which required them to finance, import, and install the LIMS at a designated place (referred to as the “**surveillance center**”) for the use of (unidentified) ‘designated agencies’.¹⁹² The TSPs also asserted that, once access was granted, they had no means to monitor or assess whether, or to what extent, the LIMS had been used by PTA or any designated agency.¹⁹³

Once installed, the LIMS enabled the interception of consumer data by allowing the designated agencies to directly tap into the network of the service providers—with the click

¹⁸³ IHC Order dated June 25, 2024, passed in the clubbed cases, available at https://mis.ihc.gov.pk/attachments/judgements/162135/3/W.P_No_2758_of_2023_638552863698115144.pdf.

¹⁸⁴ *Id.* at 2.

¹⁸⁵ *Id.* at 3.

¹⁸⁶ *Id.*

¹⁸⁷ *Id.* at ¶5-11.

¹⁸⁸ *Id.*

¹⁸⁹ *Id.* at 11.

¹⁹⁰ *Id.* at 8.

¹⁹¹ *Id.* at 12.

¹⁹² *Id.* at 13.

¹⁹³ *Id.* at 15.

of a button—by initiating a track and trace request using the unique SIM, IMEI or MSISDN number associated with the consumer’s device.¹⁹⁴ The subsequent process was entirely automatic, with the SMS, CDRs and metadata associated with the consumer being reported into a monitoring center established at the surveillance center.¹⁹⁵ Through another server, the entire content of the consumer’s communications routed through the TSP—including audio, video and search histories—would be transmitted to this monitoring center, and stored.¹⁹⁶ Any encrypted material, generated from applications like WhatsApp, that formed part of the transmitted data would also be shared with the monitoring center.¹⁹⁷ And while the LIMS itself lacked the capability to automatically decrypt such data, requests for decryption could be made to the company owning the relevant application.¹⁹⁸

It was further revealed that TSPs were required to ensure that up to 2% of their entire consumer base can be surveilled through the LIMS.¹⁹⁹ The TSPs reiterated that they had no way to monitor which consumers were being surveilled.²⁰⁰ The designated agencies could therefore access the LIMS, a mass surveillance system exposing the data of over 4 million citizens, without any supervision, oversight or control.²⁰¹

In its consequent order (the “**June 25 Order**”), the IH Court noted how, throughout the proceedings, the Federal Government, its Divisions, LEAs, and the intelligence agencies denied that any agency or entity had been authorized to undertake surveillance pursuant to the PTRAs, IFTAs and/or the Telegraph Act—the only laws providing for lawful interception—or that any rules had been made for this purpose.²⁰²

The High Court found that this gave rise to one of two possibilities: either the State, through its investigative and intelligence agencies, never deemed it necessary to conduct surveillance for any legitimate State purpose and therefore did not do so; or, alternatively, that these agencies do, in fact, engage in surveillance—but do so unlawfully, without any legal authority or oversight.²⁰³ The Court referenced numerous instances of audio leaks, beyond the subject audios, in the recent past, including the leaks referenced earlier in this article.²⁰⁴ From this the Court stated it could be logically deduced that there are surveillance mechanisms in place, and in use, enabling the recording of the highest executive, legislative and judicial officeholders of the country.²⁰⁵

The IH Court observed that this was both ‘*frightening and damning for a rule of law democracy functioning under the Constitution*’.²⁰⁶ It noted that Article 14 guarantees the right to privacy, whereas the right to life and liberty under Article 9 also includes the right of citizens to be left alone in their private spheres. The freedom of speech, guaranteed by Article 19, also includes the freedom to speak freely, without the State prying into the conversation. These constitutional guarantees had been undermined through the mass surveillance of citizens in Pakistan without any constitutional or legal backing, or judicial oversight. Justice Sattar likened this to George Orwell’s *1984*, observing that the mass surveillance system seemed to be inspired by the dystopian novel.

Relying on the judgment passed in the *Mohtarma Benazir Bhutto* case, cited earlier—and the ‘*unambiguous provisions*’ of the IFTA, Telegraph Act, PECA, PTRAs, and the relevant criminal laws—the IH Court held that any surveillance undertaken in breach of the IFTA is a

¹⁹⁴ *Id.* at 12.

¹⁹⁵ *Id.*

¹⁹⁶ *Id.*

¹⁹⁷ *Id.*

¹⁹⁸ *Id.*

¹⁹⁹ *Id.*

²⁰⁰ *Id.*

²⁰¹ *Id.* at 16.

²⁰² *Id.* at ¶¶18-22.

²⁰³ *Id.* at 23.

²⁰⁴ *Id.* at ¶¶24-25.

²⁰⁵ *Id.* at 26.

²⁰⁶ *Id.* at 28.

criminal act.²⁰⁷ To the extent that the LIMS had been installed under the direction and supervision of the State—enabling the mass, simultaneous, surveillance of over four million citizens—the liability lay with the Federal Government. The Prime Minister and members of his cabinet were held to be ‘*individually and collectively responsible*’ for the existence and operation of any mass surveillance system, if it were to turn out that such surveillance is being, or has been, undertaken.

The Court directed that its June 25 Order be placed before the Prime Minister and the members of the Cabinet, with the expectation that the Prime Minister would solicit appropriate reports from all intelligence agencies under his purview and place the matter before the Cabinet. Within six weeks, the Prime Minister was to have a report filed on behalf of the Federal Government disclosing:²⁰⁸

- (i) whether surveillance is being undertaken in Pakistan in breach of the relevant legal framework, and the fundamental rights guaranteed in Article 9, 14 and 19 of the Constitution;
- (ii) who is responsible, and to be held liable, for the installation of the LIMS in breach of this legal and constitutional framework; and
- (iii) who is in charge of operating the LIMS, and therefore to be held liable for breaching the right to privacy of citizens whose data had been accessed and released.

The TSPs were directed to file sealed reports containing the entirety of correspondence between them and the PTA with respect to the procurement, installation, and operation of the LIMS.²⁰⁹ And, given that there was no agency authorized to conduct surveillance, the Court directed all TSPs—regardless of whether they were part of the proceedings—to ensure that the LIMS is not used to procure their consumers’ data. This would, of course, have no impact on surveillance conducted for any legitimate State purpose, in accordance with the IFTA, particularly since TSPs had been directed to resume sharing information with the ICT Police, in accordance with the Ministry of Interior’s SOPs, until the next date of hearing. To the extent that any of the TSPs enabled any entity or person to illegally access citizens’ data, their management, and the members of their board of directors would be rendering themselves individually and collectively liable to criminal liabilities under the aforementioned laws.

With respect to the PTA, the Islamabad High Court stated that, in its preliminary view, the Chairman and members of the PTA had misrepresented themselves before the Court, particularly with respect to the LIMS.²¹⁰ The PTA was therefore directed to submit a sealed report, along with its correspondence with telecom licensees for the procurement, installation, and operationalization of the LIMS, while identifying how the surveillance center is manned, and which entities and individuals have access to it. Technical experts from the PTA were directed to make a graphic representation before the Court, explaining the manner in which the LIMS operates, and how data procured through the system is stored, retrieved, used, protected, and destroyed (if at all). The Court also initiated contempt proceedings against the Chairman and members of PTA.²¹¹ The Federal Government request to present documentation to the Judge in-chambers was rejected, and these documents were ordered to be filed in a sealed envelope instead.²¹²

The matter was rescheduled for September 4, 2024.²¹³

²⁰⁷ *Id.* at ¶¶29-31.

²⁰⁸ *Id.* at 32.

²⁰⁹ *Id.* at 33.

²¹⁰ *Id.* at 35.

²¹¹ *Id.* at 36.

²¹² *Id.* at 37.

²¹³ *Id.* at 39.

2. Supreme Court Intervention²¹⁴

On July 05, 2024, the Federal Government challenged the Islamabad High Court's June 25 Order before the Supreme Court. It argued that the IH Court had gone beyond the scope of the matter before it,²¹⁵ proceeding *suo motu* when there was no live issue to adjudicate, given that the Special Committee challenged by the Petitioner, Najam us Saqib, had ceased to exist.²¹⁶ Moreover, the unauthorized recording of private conversations had already been declared an offence under Section 19 of the PECA, leaving no '*no occasion*' for a declaration to this effect by the High Court.²¹⁷

Before the appeal could be heard, the Federal Government, through the Ministry of Information Technology and Telecommunication, issued a notification under Section 54 of the Pakistan Telecommunication (Re-Organization) Act, 1996 on July 08, 2024 (the "**July 8 Notification**").²¹⁸ This authorizes officers nominated by the Inter-Services Intelligence (ISI) to intercept calls and messages, or to trace calls through any telecommunication system '*in the interest of national security and in the apprehension of any offence*'.²¹⁹ Challenges against it are currently pending before several High Courts across Pakistan, including the Islamabad High Court.²²⁰

The appeal against the June 25 Order passed in the Audio Leaks Case was heard by a two-member bench of the Supreme Court on August 19, 2024, when the Federal Government informed the Court of the IH Court's May 29 Order barring telecom service providers from recording phone calls and data for surveillance purposes, except in accordance with the 2013 Investigation for Fair Trial Act. This was stated to have hindered intelligence and law enforcement agencies in probing crimes and monitoring terrorism, and prevented intelligence agencies such as the Inter-Services Intelligence and Intelligence Bureau from performing counter-intelligence activities.²²¹ The difference between the comments of the two judges was stark, with one, Justice Naeem Akhtar Afghan, expressing concern over the situation, and lamenting that, in this country, no one wants to uncover the truth.²²² On the other hand, Justice Amin ud Din Khan commented that it was possible the individuals implicated in the leaks had themselves leaked the audios, given that every mobile phone has the capacity to record calls, and questioned whether this aspect had been probed.²²³ The Supreme Court

²¹⁴ It should be noted that the orders passed in the Supreme Court proceedings were not published on the Court's website (in contravention of prevailing practice), leaving the public to rely on news media sources to gather information on the proceedings. As such, information on further proceedings in this case is limited.

²¹⁵ Terence J Signamony, *Audio leaks case: SC urged to set aside IHC order in response to pleas of Bushra, Najam*, BUSINESS RECORDER (Jul. 6, 2024), <https://www.brecorder.com/news/40311532/audio-leaks-case-sc-urged-to-set-aside-ihc-order-in-response-to-pleas-of-bushra-najam>.

²¹⁶ Hasnaat Malik, *Govt challenges IHC's leak case order*, TRIBUNE (Jul. 6, 2024), <https://tribune.com.pk/story/2477102/govt-challenges-ihcs-leaks-case-order>.

²¹⁷ Order dated June 25, 2024, *supra* note 184.

²¹⁸ S.R.O. 1005(I)/2024, dated July 08, 2024, issued by the Ministry of Information Technology and Telecommunication [8072 (2024)/Ex. Gaz.]. News Desk, *Govt. Authorises ISI to Intercept Calls and Messages for National Security*, TRIBUNE (Jul. 9, 2024), <https://tribune.com.pk/story/2478140/government-authorises-isi-to-intercept-calls-and-messages-for-national-security>.

²¹⁹

Signamony, *supra* note at 216.

²²⁰ This includes the Lahore, Islamabad and Sindh High Courts (HC(s)). In the Lahore HC: *Govt's surveillance order challenged in LHC*, TRIBUNE (Jul. 11, 2024), <https://tribune.com.pk/story/2478709/govts-surveillance-order-challenged-in-lhc>; In the Islamabad HC: *PBC also challenges surveillance order*, TRIBUNE (Jul. 12, 2024), <https://tribune.com.pk/story/2478988/pbc-also-challenges-surveillance-order>; In the Sindh HC: *Ishaq Tanoli, SHC issues notices in ISI 'interception' powers case*, DAWN (Jul. 23, 2024), <https://www.dawn.com/news/1847466>.

²²¹ Abdullah Momand, *SC suspends IHC order in audio leaks case, bars court from further proceedings*, DAWN (Aug. 19, 2024), <https://www.dawn.com/news/1853303>.

²²² Abdul Qayyum Siddiqui, *Audio leaks case: SC directs IHC to stop proceedings till further orders*, GEO NEWS (Aug. 19, 2024), <https://www.geo.tv/latest/559987-audio-leaks-case-sc-directs-ihc-to-stop-proceedings-till-further-orders>; News Desk, *Supreme Court halts Islamabad High Court proceedings in audio leaks case*, TRIBUNE (Aug. 19, 2024), <https://tribune.com.pk/story/2489238/supreme-court-halts-islamabad-high-court-proceedings-in-audio-leak-case>.

²²³ Signamony, *supra* note at 216.

ultimately restrained the IH Court from taking any further action, and suspended the IH Court's June 25 Order, effectively restoring the surveillance regime.²²⁴ There do not appear to have been any further developments in this case, though the initial two-member bench formed to hear the appeal was reconstituted into a five-member one, which excludes Justice Naeem Akhtar Afghan.²²⁵

V. Conclusion

While it appears that the Federal Government—and its extensions, including the law enforcement and intelligence agencies—may have succeeded in evading accountability *this time*, it is nevertheless important to examine the rather suspect claims made in the process, and chart a course that leads to true progress. The positions taken by the Pakistani Government are not without precedent; rather they reflect a broader global pattern, transcending the issue of surveillance, wherein national security imperatives are invoked to deflect scrutiny with respect to the use of broad discretionary powers, often at the cost of constitutional freedoms. This moment therefore offers a critical opportunity for all democratic societies to reflect more seriously on the legal and institutional safeguards we must advocate for to ensure that such powers are not exercised in ways that violate fundamental freedoms.

In Pakistan's case, the Federal Government contends that it lacks the technological capability to surveil citizens, or to identify those doing so, and had not authorized any agency or body for this purpose. The former contention is clearly contradicted by publicly available data, such as Privacy International's comprehensive special report on security and surveillance in Pakistan.²²⁶ This report reveals that Pakistan not only possesses a wealth of surveillance technologies, but has actively facilitated local intelligence agencies, and foreign states in surveilling its own citizens.²²⁷

And while it is acknowledged that the mere existence of surveillance capability, does not, on its own, prove culpability; it does raise urgent questions about oversight, access controls, and the *potential* for abuse—whether by rogue officials, '*hostile agencies*', or state institutions themselves. In any jurisdiction, the unchecked capacity to collect and retain personal data opens the door to misuse, even when deployed to meet admittedly legitimate objectives, such as national security or criminal justice. Following the issuance of the July 08 Notification, granting the Inter-Services Intelligence (ISI) broad-based powers of surveillance, this potential for abuse has increased considerably. The military-run ISI is left to determine the boundaries of vague and obscure terms such as '*national security*', and the '*apprehension*' of an offence.

What emerges from the Audio Leaks Case, therefore, is not necessarily a conclusive finding of state complicity but, perhaps, a deeper institutional failure: either to prevent abuse of power, or to ensure that objectives of national security and criminal justice are met in a proportionate manner and made subject to democratic oversight and legal accountability. We have seen that in the absence of such safeguards, breaches of digital privacy stand to inflict irreparable harm on the reputations, liberties, and safety of individuals—from ordinary citizens to politicians—often without the procedural protections of due process. These harms reverberate throughout the democratic system, deterring the freedom of expression, quelling dissent, and undermining the integrity of core institutions, including the judiciary. A society stricken by the fear of such harm can never truly be free.

To facilitate meaningful progress, we must therefore move beyond critique and commit to concrete, actionable reforms. What follows is an attempt to do just that, by proposing

²²⁴ *Id.*

²²⁵ Web Desk, *SC forms Five-Member bench to hear audio leaks case*, THE NATION (Sep. 23, 2024), <https://www.nation.com.pk/23-Sep-2024/sc-forms-five-member-bench-to-hear-audio-leaks-case>.

²²⁶ *Tipping the scales: Security & surveillance in Pakistan*, *supra* note 15.

²²⁷ *Id.*

targeted legislation and amendments to the existing legal framework designed to minimize the risk of misuse, manipulation, or even negligent oversight of surveillance powers.

(i) Harmonizing Statutes

Which statute wins?

In Pakistan, the unresolved discord between key statutes governing the interception of information, particularly the Pakistan Telecommunication (Re-Organization) Act, 1996 (the PTRA), and the Investigation for Fair Trial Act, 2013 (the IFTA), heightens the risk of Pakistan's surveillance framework being abused, leaving loopholes that can be exploited by those for whom the lack of data security represents an opportunity, rather than a liability.

From the discussion in the earlier chapters, it is evident that the scope of 'lawful interception' is far broader under the PTRA—specifically Section 54 (1) of the Act—which allows the Federal Government to authorize an officer to intercept calls and messages, or trace communications, on the ground of national security, or in the apprehension of any offence. The IFTA, was passed specifically to counter the arbitrariness of intelligence and law enforcement agencies in intercepting data and conducting surveillance. To this end, the IFTA lays out a detailed mechanism for obtaining a warrant, as previously described, and limits the purposes for which such a warrant can be sought to offences pertaining to terrorism.

However, Section 54 (1) of the PTRA contains what is known as a *non-obstante clause*, meaning it applies '[n]otwithstanding anything contained in any law for the time being in force', and therefore has an overriding effect over other laws. The IFTA, too, has an overriding effect, by virtue of Section 38 of the Act. According to settled legal principles, applicable in numerous jurisdictions, where two conflicting statutes cannot be harmonized, as in this case, it is ordinarily the statute later in time that prevails. However, this is subject to a host of other factors, such as the object, purpose and policy undergirding both statutes, and the legislative intent communicated through their language.²²⁸

As such, there is no clarity regarding the interaction of the PTRA and the IFTA, though common sense may demand it be the latter that prevails based on the clearly expressed intention of the legislature. During the Audio Leaks Case, Justice Sattar had commented that any rules made to regulate the authorization and conducting of surveillance under Section 54 of the PTRA would necessarily have to be in compliance with the IFTA, however, this does not settle the matter.²²⁹ There is therefore an urgent need for the legislature or the superior judiciary to resolve this issue as, presently, Section 54 of the PTRA provides a means to circumvent, and render redundant, the elaborate procedure and safeguards laid out under the IFTA. The July 08 Notification empowering the ISI to conduct surveillance, while bypassing the need for a judicial warrant under the IFTA, is clear evidence of this glaring flaw in Pakistan's legal framework.

(ii) Accountability, Safeguards and Specific Legislation

When is interception 'lawful'?

There is also a need to narrow the boundaries of what constitutes 'lawful' interception or surveillance. In Pakistan, the IFTA achieves this goal through the use of clear language, and provisions to prevent and punish the misuse of surveillance frameworks. However, as previously mentioned, the beneficial effects of the IFTA are neutered by Section 54 of the PTRA, which employs far broader language, including vague references to '*national security*', and does not contain any mechanism to punish such abuse. It is this disharmony

²²⁸ This has been held by the superior judiciary in a number of judgments, such as the Supreme Court's in *Syed Mushahid Shah and others v. Federal Investment Agency and others*, reported as **2017 SCMR 1218**, available at https://www.scp.gov.pk/files/judgments/C.A._2561_2016.pdf.

²²⁹ ¶17 of Order dated June 25, 2024, which now stands suspended, *supra* note 182.

that enabled the Federal Government to issue the July 08 Notification. Following this notification, no individual warrants will have to be sought, and the Federal Government may authorize surveillance at its discretion, without being bound by the provisions of the IFTA. The ISI, in turn, will have unfettered access to Pakistan's surveillance infrastructure, likely with little to no oversight.²³⁰

With no safeguards to mitigate excesses, it is impossible to predict the extent of intrusive surveillance Pakistani citizens will be subjected to under the guise of '*national security*'. This controversy can only be resolved through the legislative process, or by the judiciary, which can exercise its powers of judicial review to harmonize the PTRa with the IFTA, or, alternatively, to invoke Article 8 of the Constitution and strike down the portions of the PTRa deemed inconsistent with fundamental rights.

The need for a personal data protection bill

But, beyond this, there remains a dire need to supplement the existing legislative framework with a comprehensive personal data law. This is particularly crucial, given there is currently no legal framework to regulate the interception, use, collection, storage and disclosure of personal data by the government, organizations and other individuals and entities in Pakistan. While the Ministry of IT&T proposed a Personal Data Protection Bill for this purpose in 2023, the Bill was subjected to great criticism for ambiguities lending themselves to exploitation.²³¹ But despite the barrage of audio leaks seen in 2023, this Bill has yet to be debated or passed into law.

There is therefore a critical need to design effective legal mechanisms to detect and punish the misuse of personal data, both by domestic and foreign entities. The framework in the European Union (EU) provides a useful model, incorporating both reactive and pre-emptive measures for data protection, while empowering individuals to monitor the collection of their data. The EU's data protection legislation comprises the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), and the Data Protection Regulation for EU institutions, bodies, offices and agencies (EUDPR).²³²

The GDPR, for example, establishes binding principles for the lawful processing of personal data, including requirements of purpose limitation, data minimization, transparency, and explicit consent.²³³ It applies to the private sector, as well as a majority of public sector entities, and enables individuals to access their own (collected) data, while keeping them informed on how it is being processed.²³⁴ It also provides individuals with the '*right to be forgotten*', allowing their data to be deleted where they see no legitimate reason for its retention; and the right to know when the security of their personal data has been breached.²³⁵ Additionally, public authorities, and organizations that process data on a large scale, or whose core activity is the processing of special categories of data, are obligated to designate Data Protection Officers (DPOs) under the GDPR.²³⁶ These DPOs advise on compliance with data

²³⁰ This is evident from the earlier statement by the Prime Minister's Office that they do not interfere with the operational affairs of the Inter-Services Intelligence (ISI) agency during the Audio Leaks Case, *supra* note 134.

²³¹ *Privacy International raises concerns regarding Pakistan's Personal Data Protection Bill*, Privacy International (Aug. 8, 2023), <https://privacyinternational.org/news-analysis/5090/privacy-international-raises-concerns-regarding-pakistans-personal-data>.

²³² *Legal framework of EU data protection*, European Commission, https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en.

²³³ *What are the main aspects of the General Data Protection Regulation (GDPR) that a public administration should be aware of?* European Commission, https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en.

²³⁴ *Summary, General Data Protection Regulation*, European Commission, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:310401_2.

²³⁵ *Privacy International raises concerns regarding Pakistan's Personal Data Protection Bill*, *supra* note 232.

²³⁶ *Id.*

protection rules, and facilitate compliance, while acting as intermediaries between the supervisory authorities, data subjects, and the organization or authority by which they have been appointed.²³⁷ Such public and private entities are also required to document and record their processing activities.²³⁸

The GDPR also empowers individuals to lodge a complaint with a supervisory authority where the processing of their personal data is alleged to have infringed the GDPR. It also entitles individuals to compensation for any material or non-material damage suffered as a result of such infringement,²³⁹ and empowers the supervisory authority to impose administrative fines with respect to such infringement, commensurate with the gravity thereof.²⁴⁰ For instance, in 2023, Meta, the parent company for Facebook, was issued a 1.2 billion euro fine by the Irish Data Protection Authority for its infringement of GDPR provisions pertaining to data transfers.²⁴¹

The EUDPR creates similar rights and obligations with respect to EU institutions, bodies, offices and agencies.²⁴² The LED, on the other hand, regulates the processing of personal data connected with criminal offences or the execution of criminal penalties.²⁴³

Invalidating and Deterring Data Misuse

Lastly, it is essential to ensure that unlawfully obtained digital content is not admissible in judicial, disciplinary, or administrative proceedings, or allowed to influence such proceedings, whether directly or indirectly, especially where it infringes upon the fundamental right to privacy. Institutions cannot operate with integrity when their internal dynamics are susceptible to manipulation through illegitimate digital disclosures. Moreover, using such material to punish or discipline individuals sets a dangerous precedent: one which legitimizes unlawful surveillance and encourages its use. This practice must be unequivocally rejected, not only by those targeted, but by society as a whole.

(iii) Demanding Compliance with International Obligations

Pakistan is one of numerous countries that has signed and ratified the International Covenant on Civil and Political Rights (ICCPR), Article 17 of which obligates state parties to safeguard data privacy.²⁴⁴ Article 28 of the ICCPR establishes the Human Rights Committee (HRC), a body of eighteen independent experts tasked with monitoring the implementation of the ICCPR by States Parties.²⁴⁵ To this end, the HRC is required to scrutinize periodic reports submitted by States Parties on the measures adopted to give effect to the rights recognized in the ICCPR, and provide its comments.²⁴⁶

²³⁷ *Id.*

²³⁸ *Id.*

²³⁹ Article 82, GDPR, <https://gdpr-info.eu/art-82-gdpr/>.

²⁴⁰ Article 83, GDPR, <https://gdpr-info.eu/art-83-gdpr/>.

²⁴¹ *1.2 billion euro fine for Facebook as a result of EDPB binding decision*, European Data Protection Board, https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

²⁴² *Legal framework of EU data protection*, *supra* note 2333.

²⁴³ *Id.*

²⁴⁴ Article 17, *International Covenant on Civil and Political Rights* [ICCPR], Office of the United Nations High Commissioner for Human Rights (adopted Dec. 16, 1966), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>. Please note that Article 17 does not expressly use the term ‘data privacy’, however the United Nations General Assembly’s Resolution 68/167 emphasizes that the unlawful or arbitrary surveillance and/or interception of communications, or collection of personal data, are highly intrusive acts, violating the rights to privacy and freedom of expression. See Jannat Ali, *A Data Protection Law in Pakistan: Policy Recommendations by DRF*, Digital Rights Foundation (Oct. 13, 2017), <https://digitalrightsfoundation.pk/data-protection-law-in-pakistan-policy-recommendations-by-drf/>.

²⁴⁵ *Human Rights Committee*, Office of the United Nations High Commissioner for Human Rights, <https://www.ohchr.org/en/treaty-bodies/ccpr>.

²⁴⁶ States Parties are mandated to submit periodic reports in this regard under Article 40 of the ICCPR. See ICCPR, *supra* note 245.

On December 02, 2024, the HRC issued its concluding observations on Pakistan's second periodic report wherein it specifically expressed concern regarding the July 08, 2024 notification authorizing the ISI to intercept calls and text messages of citizens under Section 54 (1) of the PTMA, as well as the installation of the Lawful Intercept Management System (LIMS) which was a focal point in the Audio Leaks Case.²⁴⁷ The HRC also expressed concern regarding reports of the targeted surveillance and monitoring of individuals such as human rights defenders, journalists, political activists, politicians and individuals critical of the government through various means, including the use of digital technologies such as spyware. In view of these developments, the HRC recommended that Pakistan promptly adopt a comprehensive data protection law that ensures transparency, accountability and protection of data privacy in line with international human rights standards, while complying with the principles of '*legality, proportionality and necessity*'. It called for the establishment of independent oversight mechanisms, including the independent and impartial judicial review of surveillance activity, and to ensure access to effective remedies. Unfortunately, the HRC lacks the coercive power to enforce these crucial recommendations, making it all the more important to ensure sustained public pressure within Pakistan—from individuals, civil society and human rights organizations alike—to comply with these recommendations, and honor its international obligations under the ICCPR.

While Pakistan's failure to confront the fallout of its recent digital scandals represents a missed opportunity for reform; on a global scale, its experience demonstrates the urgent need for comprehensive data protection laws that both prevent and punish invasions of privacy and are insulated from political interference. In fragile democracies and mature legal systems alike, unchecked surveillance and politicized data breaches threaten to compromise institutional independence, derail accountability mechanisms, and fundamental freedoms—striking at the very foundations of justice. Upholding the sanctity of privacy is therefore not merely a matter of personal liberties, but a collective imperative—to preserve the integrity of democratic institutions and uphold the rule of law. As digital intrusions grow more sophisticated and pervasive, the task for the global community is clear: to build resilient legal frameworks capable of withstanding manipulation and protecting the democratic values they claim to uphold.

However, our success in this regard presupposes the existence of a rule of law regime; one where the various branches of the State remain confined to their spheres and abide by both the letter and the spirit of the law. It also requires meaningful compliance by private organizations and entities which are bound by international principles and obligations to safeguard consumer data, such as under the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR). These international instruments now stand enshrined in principles laid out by the Global Network Initiative, which was launched in 2008 to protect and advance the freedom of expression and privacy rights, by setting global standards in the information and communication technologies (ICT) sector to regulate decision-making in the face of government restrictions and demands.²⁴⁸ The GNI comprises internet platforms, telecommunication operators, equipment vendors and other entities playing a key role across the ICT sector.²⁴⁹ The role of private organizations and entities is thus of great importance, as compliance with illegal surveillance requests has the potential to do grave damage to the existing surveillance framework in Pakistan, and in other jurisdictions. It is worth noting that, in the face of the Government's denial of any lawful, state-authorized surveillance, whether in the form of the

²⁴⁷ Human Rights Committee, *Concluding observations on the second periodic report of Pakistan* (CCPR/C/PAK/CO/2), at ¶44, Office of the United Nations High Commissioner for Human Rights, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2F2002/22&Lang=en.

²⁴⁸ *The GNI Principles at Work: Public Report on the Fourth Cycle of Independent Assessments of GNI Company Members 2021/2022*, Global Network Initiative, https://globalnetworkinitiative.org/wp-content/uploads/2023/10/GNI_PAR23_.pdf.

²⁴⁹ *Human Rights Committee*, *supra* note 246.

Lawful Intercept Management System (LIMS) or otherwise, service providers that allowed any agency, individual or other entity to utilize their technical facilities of interception prior to the July 8 Notification would have been acting in violation of Section 17 (2) of the Investigation for Fair Trial Act, 2013.

Lastly, as individuals what we can do is to fulfil a more fundamental duty: to reject vague denials, institutional silence, and the normalization of unchecked surveillance, wherever we may be. We must demand that our governments uphold their constitutional commitments and international obligations with respect to the freedom of expression, and the rights to privacy and due process, regardless of our personal affiliations or political leanings. Ultimately, we must recognize that when the rights of even one individual are compromised, the rights of all are endangered.