UCP Journal *of* Law & Legal Education
Vol. 3, Issue 2 (January – June 2025)

Privacy and Surveillance: Legal and Technical Perspectives

Arifa Naheed Rana*, Amina Iqbal*

Abstract

Privacy and surveillance pose complex challenges at the intersection of law, technology, and human rights. In Pakistan, constitutional guarantees such as Article 14 safeguard individual dignity and privacy, yet existing statutes and institutional practices remain fragmented and fall short of international standards. This paper addresses this gap by conducting a doctrinal and comparative legal analysis of Pakistan's surveillance framework, focusing on the Investigation for Fair Trial Act 2013, the Prevention of Electronic Crimes Act 2016, and related judicial precedents. Using necessity, proportionality, legality, oversight, and remedies as evaluative rubrics, the study finds that Pakistan's current framework permits broad executive discretion, lacks adequate judicial oversight, and struggles to balance state security with civil liberties. The paper contributes by proposing structured reforms, including codified warrant procedures, independent oversight mechanisms, and a staged national AI and cybersecurity strategy to align Pakistan's legal framework with global human rights standards.

Keywords: Cybercrime, Cybersecurity, Privacy, Protection, Surveillance,

Introduction

This article addresses the legal, ethical, and technical aspects of privacy and surveillance, highlighting the obstacles and responsibilities encountered by both technology engineers and law enforcement agencies.

This article has been meticulously crafted to address constitutionality and societal implications of surveillance primarily through a human rights lens. This indicates that surveillance

*****Senior Lecturer, Faculty of Law, Capital University of Science and Technology Islamabad, Pakistan. email: arifa.naheed@cust.edu.pk
******Lecturer, Faculty of Law, Capital University of Science and Technology, Islamabad, Pakistan. email: amina.iqbal@cust.edu.pk
Article History: Received: 13 May 2025; Received in revised form: 26 August 2025; Accepted: 08 October 2025.
Available online: 20 October 2025
DOI: https://doi.org/10.24312/ucp-jlle.03.02.552

conducted by both state and non-state entities can profoundly impact the freedoms inherent in a democratic society, and its implementation without appropriate safeguards may lead to concerning repercussions for those liberties (Cukier, 2021). Mohana, in his 2018 article, *Ways of Being, Seen: Surveillance art and the Interpellation* of *Viewing Subjects*, wrote that wiretapping encompasses the clandestine electronic surveillance and interception of telephonic, facsimile, or alternative communication methods. This technology originates from the 19th century and has played a pivotal role in the government's efforts to combat organised crime (Monahan, 2017). Subsequently, various electronic surveillance techniques emerged during the Cold War period (Monahan, 2017). Conversely, cyber surveillance represents a contemporary counterpart to wiretapping; it observes individuals utilising 'smart' devices that rely on a data network for communication (Monahan, 2017). He further states that this modern approach to surveillance encompasses virtually all telecommunication systems, encroaching upon individual liberties. Pakistan has ratified and signed multiple instruments that address the right to privacy. These instruments relate to the concealment or obscuration of aspects of one's life from the public at large.

International law affords significant protection through instruments such as the ICCPR (International Covenant on Civil and Political Rights) and UDHR. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the ICCPR stipulate that individuals must not face arbitrary or unlawful intrusions into their privacy, domicile, familial relations, or communications (UN General Assembly, 1948). Moreover, international law provides essential safeguards to mitigate such interventions and/or attacks (ICRC, 2019). The legal regulation of such interruptions holds significant importance, as articulated in the General Comment to Article 17: 'There has to be legislation that governs how public and commercial entities collect and store personal data on computers, databases, and other devices (United Nations Human Rights Committee, 1988).' Additionally, territorial frameworks, for example, the ECHR (European Convention on Human Rights) and the EU, have repeatedly affirmed the importance of data protection and the right to privacy (Council of Europe, 1950). This proves that protecting personal information is of utmost significance to everyone.

As a basic right, the right to privacy is also firmly embraced and protected by Pakistan's constitution. The right to personal autonomy and the right to live in peace are guaranteed in Article 14. In *PLD 2023 SC 461* (Supreme Court of Pakistan, 2023), the Court held that, the right to privacy is a prerequisite for individual autonomy, a primary aspect of the right to liberty and right of life, and, most importantly, 'attaches to the person, not to the place where it is associated,' according to Pakistan's highest court. In this context, this research examines how Pakistan's key surveillance laws, specifically the Prevention of Electronic Crimes Act (PECA) 2016 and the Investigation for Fair Trial Act (IFTA) 2013, align with the necessity and proportionality standards enshrined in Article 17 of the ICCPR. In doing so, it asks what statutory and institutional reforms could better align Pakistan's privacy and surveillance framework with international human rights benchmarks while maintaining operational effectiveness, and how oversight, transparency, and remedies within Pakistan's cybersecurity governance can be strengthened to provide stronger protections for civil liberties.

This paper demonstrates that Pakistan's data privacy legislation is not in alignment with international standards. It also highlights the need to establish robust frameworks to address the escalating cybercrimes and the limitations of current cybersecurity measures. The article emphasises the need for alternative legislative processes that respect civil liberties by identifying a conflict between state security and individual privacy rights. It necessitates enhanced collaboration between the public and private sectors to fortify cybersecurity infrastructure and protect personal data.

Methodology

This study employs a doctrinal legal research approach combined with comparative benchmarking. The analysis draws on Pakistan's constitutional framework, particularly Article 14 of the Constitution of 1973, and key statutes including the Pakistan Telecommunication (Reorganisation) Act 1996 (s.54), the Investigation for Fair Trial Act 2013, and the Prevention of Electronic Crimes Act 2016. Leading judicial precedents, such as Benazir Bhutto v. Federation of Pakistan (1998) and Shehla Zia v. WAPDA (1994), as well as recent Islamabad High Court rulings,

are also examined. Secondary sources include academic literature, government reports, and NGO publications. The corpus covers materials from 1994 to 2024, selected for their relevance to privacy, surveillance, and cybersecurity governance. Evaluation is conducted using five rubrics: necessity, proportionality, legality, oversight, and remedies derived from international human rights standards, particularly Article 17 of the ICCPR and the "Necessary & Proportionate" Principles. This methodological framework enables a systematic identification of compliance gaps and the development of targeted policy recommendations.

Literature Review

Academic and judicial commentary consistently emphasise that Article 14 of the Constitution of Pakistan, 1973, enshrines dignity and privacy as fundamental rights. Internationally, Article 17 of the ICCPR and Article 12 of the UDHR affirm similar protections (UN, 1966; UNGA, 1948). Scholars argue that Pakistan's courts have progressively recognised privacy as extending beyond the home into personal communications and digital data (Richards, 2013). So what? This constitutional recognition provides a strong foundation, yet statutory frameworks and executive practices have lagged.

The Investigation for Fair Trial Act (2013), the Prevention of Electronic Crimes Act (2016), and S.54 of the Pakistan Telecommunication Act (1996) form the legal basis of surveillance. Literature highlights that these laws confer wide discretion on intelligence agencies, often without adequate safeguards (Privacy International, 2019; Sami, 2024). Cases such as Benazir Bhutto v. Federation of Pakistan (1988) further underscore how unchecked surveillance undermines fundamental rights. So what? While statutory authority exists, it often conflicts with constitutional protections and lacks precise definitions of "national security" or "public interest."

It has been noted that Pakistan lacks strong institutional oversight mechanisms compared to jurisdictions such as the EU or the ECHR system (Alam & Warraich, 2024; Aftab, 2024). Judicial authorisation under IFTA (Investigation of Fair Trial Act) is limited and often discretionary, while independent review bodies remain absent (UNHRC, 2019). Empirical studies point to misuse of PECA

for silencing dissent and targeting journalists (Aziz, 2018). So what? Oversight gaps allow executive overreach, weakening trust in state institutions and undermining democratic governance.

Comparative literature emphasises that effective surveillance regulation requires necessity, proportionality, and legality as tested under the ICCPR and the "Necessary & Proportionate" Principles (OHCHR, 2014). The EU's GDPR and regional frameworks provide models of codified warrant standards, notification rights, and appeal mechanisms (European Union, 2016). So what? Benchmarking against these standards highlights the reform deficit in Pakistan's system, setting the stage for recommendations.

Taken together, the literature reveals a persistent gap: Pakistan recognises privacy as a constitutional right but has failed to institutionalise safeguards that match global standards. This gap frames the central contribution of this paper, assessing Pakistan's surveillance laws against necessity and proportionality principles and proposing reforms to align them with international human rights law.

Legal Framework of Privacy in Pakistan

Legal Framework beyond causes; Governments are undertaking surveillance beyond traditional legal justifications. They collect a large amount of information on their citizens with the aid of data mining tools to identify people of interest (Amicelle, 2022). A 'digital tsunami' of information about individuals is produced through modern technologies (Amicelle, 2022). The Constitution of Pakistan safeguards the right to privacy as a basic right. 'The dignity of man and, subject to law, the privacy of home, shall be inviolable,' states the Constitution in Article 14(1). According to the Constitution, this right is intended to take priority over any national legislation that may be in contradiction with it because it is a crucial basic right. According to Article 8 of the Constitution, if a regulation, tradition, or practice that is legally binding conflicts with those rights that are guaranteed by the Constitution, then it will be void to the degree that it conflicts. Article 8 (5) states clearly that '[t]he rights conferred by this Chapter shall not be suspended except as expressly provided by the Constitution.' The constitution provides strong safeguards against

the derogation of fundamental rights. (Constitution of the Islamic Republic of Pakistan, 1973).

Defining Cybersecurity

Before advancing further, it is essential to delineate key terms pertinent to cyber studies, like Cyber, Cybersecurity, and cybercrime, to provide a more professional analysis of the issues and enhance readers' comprehension of these ideas. The word 'cyber' conjures images of the internet; nevertheless, the term refers to two distinct things: online communications and electronic media (Fang, 2018). Cyber refers to communication via electronic medium (Futter, 2016). In the realm of 'Cybercrime' language, beyond legal contexts, it includes other activities, such as traditional computer offences and network-related crimes (Gercke, 2012). The dominant definition of cybercrime includes any action in which computers or systems function as a means, objective, or setting for unlawful behaviour (Gercke, 2012). The United Nations (UN) contends that a universally accepted definition of cybercrime is lacking; nonetheless, it broadly categorises it into cyber-enabled offences, cyber-dependent offences, and, precisely, online child abuse and sexual exploitation (UN Office on Drugs and Crime, 2013).

Cybersecurity Landscape in Pakistan

Pakistan, being an emerging nation around the globe, attained internet accessibility in the early 1990s and currently ranks as the tenth highest population of internet users globally (Kemp, 2020). The nation's digital economy is classified tenth according to UN criteria, and with the introduction of 2G and 4G technology, internet penetration increased to 17.8% in 2016 (Statista, 2024). According to the Pakistan Telecommunication Authority (PTA), the total number of broadband subscribers is projected to be 147 million, with a significant portion being mobile broadband users at 143 million in 2025 (PTA, 2024). It stands at 40.95% with 87 million customers, while tele density is 80.01% with 169 million cellular subscribers (PTA, 2024). As of now, 54% of the nation's population has access to mobile broadband, while mobile internet penetration is at 26% (GSMA, 2024). Given the vast population using communication and information technology, cyberspace has developed as a new area, presenting concomitant difficulties for

cybersecurity legislation (GSMA, 2024). A report published in 2018 by GCI (Global Cyber Security Index Report) has rated Pakistan as 79th worldwide for cybersecurity (International Telecommunication Union, 2024). During 2018, Pakistan was among the top five areas with the highest malware encounter rates, recording 29.51% (Microsoft, 2018). Notably, Pakistan was among the five nations with the highest cryptocurrency mining encounter rates in 2018, an impressive proportion of 1.47 (Microsoft, 2018). In 2019, a hacking incident occurred in which the mobile phones of prominent Pakistani officials were compromised via WhatsApp using a specialised virus known as 'Pegasus' (Qadeer, 2020). Concerns about this event intensified when reports surfaced indicating that Indian intelligence utilised the same software for domestic surveillance on attorneys, politicians, and others (Qadeer, 2020). Pakistan is a primary target of monitoring by the US National Security Agency (Qadeer, 2020).

According to *The News* (2018), the country's banking industry is no exception. It also confronts significant cyber risks. Card skimming, ATM card abuse, hacking, and internet payment fraud are the most prevalent phenomena (The News, 2018). Between 8,000 and 10,000 of the 25 million bank accounts are targeted by hackers within the corporate sector (Malik, 2019). The banks incurred substantial financial losses as a result of cyberattacks (Iqbal, 2021). The establishment of cybersecurity regulations in Pakistan is currently beset by the formidable obstacle of their actual execution (Andrejevic, 2014). Along with other imminent concerns, such as the existence of antagonistic intellect linkages and anti-state groups, the inadequate institutional structure in Pakistan is a significant obstacle to the execution of cybersecurity regulations (Andrejevic, 2014). Following this, we will go into the history of cyber legislation, the dynamics of Pakistan's cybersecurity law implementation, potential problems, solutions, and next steps.

Cyber Regulation in Pakistan

Over time, Pakistan's cyber regulations have developed. In 2002, the country passed its first cybercrime law, the ‘Electronic Transactions Ordinance’ (ETO). Its stated goal was to ‘accredit certification service providers and recognise and ease electronic documents, records, data, public services, and dealings (Electronic

Transactions Ordinance, 2002).' In *Akhter Hamid Ghori v. Saima Estate Developers, 1989 CLC 2173,* it was held that it only dealt with a handful of offences. It was seen as an important landmark in cybercrime legislation (*Akhter Hamid Ghori v. Saima Estate Developers*, 1989 CLC 2173). After reviewing the ETO, 2002, the Pakistani government's Ministry of Information and Technology adopted the 'Electronic Crimes Act' in 2004 to address cybercrimes such as cyberstalking, cyber fraud, cyber war, data damage, spoofing, cyberterrorism, and punishments for these offences (Iqbal, 2021). The proliferation of cybercrime in the country necessitated the passage of robust anti-crime laws as time went on. After that, 'The Prevention of Electronic Crimes Ordinance, 2007' was issued by General Pervez Musharraf, who was Pakistan's president at the time (Munir, 2010). Alternatively, this law was in its early stages and addressed just a subset of the e-crimes that were already in existence. On three separate occasions in May 2008, February 2009, and July 4th, 2009, a similar regulation was put into effect by executive decree (Sayyed & Aamir, 2021). Nonetheless, constitutional constraints prevented the Ordinance from being considered by parliament, and it expired as a result (Zahid, 2020). In response to Edward Snowden's disclosures on the US National Security Agency's web-based espionage activities in Pakistan, the Defence Committee proposed the "Seven Points Action Plan" through the head of the Senate Committee (Senate of Pakistan, 2013). To safeguard the nation's critical infrastructure, the Senate Action Plan laid forth a plan that was crucial in developing the national cybersecurity agenda (Waqar & Khan, 2020). The GOP (Government of Pakistan) announced the historic National Action Plan (NAP) at the end of December 2014 to confront terrorist operations; nevertheless, this was inadequate and included a clause on online radicalisation (Iqbal, 2021).

Before Pakistan's National Assembly passed cybersecurity legislation on 11 December 2016, leading to the creation of the Prevention of Electronic Crimes Act (PECA), 2016, the steps taken by the GOP at different points in time were temporary and did little to aid the law enforcement agencies and Judicial systems in dealing with the threat of cybercrime (Daily Times, 2024). It took MPs, cyber specialists, and key industry executives 18 months to deliberate on the bill's design before it was passed, and as we'll see in the paragraphs that follow, many parts of the law are still

contentious (Sami, 2024). Protecting vital data and information systems during transmission, preventing their unauthorised access or interception, and taking other similar precautions are also part of the legislation. The elimination of cyberstalking, cyberterrorism, hate speech, electronic fraud, spamming, spoofing, online glorification of offence, and other related crimes is also a goal of these provisions (Sami, 2024). The cyber restrictions in Pakistan are so inadequate that anyone with even basic computer skills may readily circumvent them (Sami, 2024).

Electronic Surveillance Laws and Their Implications

Pakistan has several statutes that govern the monitoring of electronic communications, including the Investigation for Fair Trial Act (2013). Digital Rights Foundation (2020) examined the *Investigation for Fair Trial Act, 2013* and noted that, the IFTA was established in February 2013 with the stated purpose of 'to provide examination for gathering of evidence using devices and current systems to prevent and efficiently deal with scheduled offenses and to control the powers of the intelligence and law enforcement agencies for matters connected therewith.' This purpose is supported by the Act itself. To keep the country safe, the law essentially made it lawful to spy on individuals and their electronic devices (Government of Pakistan, 2013).

However, human rights groups were quick to point out that this gave authorities too much leeway to abuse their authority over ordinary people (Digital Rights Foundation, 2020). The PECA, after several iterations, finally made it through the National Assembly and Senate. There were four main revisions to the bill, and several of the most significant objections remained unanswered (Digital Rights Foundation, 2020). Digital Rights Foundation also claims that Cyberstalking, harassment, hate speech, and electronic fraud are among the 28 offences covered by the Act. Additionally, service providers are required to preserve traffic data for at least one year, unless otherwise specified by the Federal Investigation Authority (FIA). Examining PECA and its implementation structures in further detail exposes the government's incompetence and reluctance to enhance internet safety, going beyond the rhetoric (Government of Pakistan, 2016). The administration now has a lot of room to mince words and intimidate political opponents thanks

to the Act (Dawn, 2024b). A concerning number of detentions and arrests of political opposition parties and their social broadcasting wings have come to pass, confirming many of the concerns voiced by digital rights campaigners (Dawn, 2024b). On suspicion of making 'anti-state' remarks online, journalists have been detained and interrogated (Dawn, 2024a). In addition, the country's inhabitants' freedom of expression has been severely limited due to the criminalisation of defamation under section 20 (offences against the dignity of a natural person (Dawn, 2024b). Moreover, in the Acts mentioned earlier, each long-distance and worldwide facilities provider is required to set up a structure that records and monitors network traffic in real-time according to section 4 of the Monitoring and Reconciliation of Telephony Traffic Regulations, 2010 (Sami, 2024).

According to the Electronic Frontier Foundation, 2014 report, however, there is still some wiggle room for exceptions, because the ban on such conduct is not comprehensive on a global or national level. Any intervention, however, must be authorised by law and must adhere strictly to the rules of necessity and proportionality to come within the legitimate scope of international law (Electronic Frontier Foundation, 2014). It is disappointing that there are so many loopholes in national legislation that allow law enforcement to avoid protecting basic rights (Electronic Frontier Foundation, 2014). Accordingly, the landscape given above is infamously fractured along general lines like 'national or public security' and 'public interest,' and it is also lacking in the essential commitment needed to meet the standards of extraordinary use of surveillance methods (Electronic Frontier Foundation, 2014). When it comes to technical definitions, the phrases 'public interests' and 'national security' may mean whatever the mind can conjure up. The Pakistan Telecommunication Act of 1996 grants intelligence personnel the authority to conduct wiretapping without previous judicial clearance, based on the grounds of national security, which are derived from the legal notice approved by the federal government of Pakistan (Dawn, 2024). The parent act of the notice must not define 'national security,' leaving it open to interpretation following the nefarious objectives of individuals in authority (Pakistan Telecommunication: Reorganization Act, 1996, s. 54). In most contexts, though, the ability of a state to safeguard its territory and independence is what is meant when people talk of national

security (IJRHSS, 2015). Problems that threaten the integrity and sovereignty of states are inevitable, but there is a method for handling them, especially when they adhere to the principles of necessity and proportionality (Electronic Frontier Foundation, 2014). Neither the necessity of the intrusions nor the nature of the national security concerns has been specified in the legal notice, nor is it reasonable to infringe on the privacy of millions of people over an ill-defined and unsubstantiated national security threat. Pakistan has violated the principles of need and proportionality in its notice by allowing wiretapping, as is shown by the presence of less stringent measures (Electronic Frontier Foundation, 2014). The notice in issue has violated the norms of international law, and its legitimacy is still up for debate, if not outright denied, as was previously established (Dawn, 2024). When it comes to matters of cyber monitoring and wiretapping by intelligence and/or law enforcement organisations, this is the opinion that the higher courts have held for many years. In the case of Benazir Bhutto, a former prime minister, the fundamental premise of the unconstitutionality of such measures was demonstrated by the sanctioning of unlawful phone tapping and other eavesdropping tactics, which violated the right to privacy (*Benazir Bhutto v. Federation of Pakistan*, PLD 1998 SC 388).

The Fair Trial Act, PECA, the Telegraph Act, and the Telecommunication Act have all outlawed the longstanding practices which are vital to the efficient operation of the legal system and the rule of law. The importance of monitoring in the battle against crime cannot be overstated. But it's illegal and unconstitutional for the government to use it as it wants. The aforementioned statutory framework and the recent ruling from the Islamabad High Court both point to this (Pakistan Telecommunications Authority, 2019). In 2014, the Electronic Frontier Foundation, Requests for monitoring cannot be granted at the discretion or whim of a judge of the High Court, as is required by national legislation. Therefore, the government's notice is obviously outside its authority, contrary to the constitution, precedents set by higher courts, and rules necessary for the rule of law (4).

Discussion

The findings demonstrate a significant tension between Pakistan's constitutional commitment to privacy and the broad discretionary powers granted to state agencies. The absence of clear definitions and safeguards allows surveillance to be justified on vague grounds of national security, leaving citizens vulnerable to rights violations.

From a governance perspective, the lack of independent oversight erodes public trust and risks politicisation of surveillance powers. The use of PECA provisions against journalists and political dissenters illustrates how security laws can be weaponised, undermining democratic accountability.

Comparatively, international benchmarks such as the ICCPR, the Necessary & Proportionate Principles, and the GDPR emphasise precision, transparency, and independent review. Pakistan's framework diverges sharply, revealing the need for statutory reform and institutional redesign.

Feasibility also emerges as a key concern. Reforms must balance civil liberties with genuine security needs. Establishing a National Cyber Coordination Centre with judicially supervised warrant procedures and annual transparency reporting could provide both legitimacy and operational effectiveness.

Ultimately, these results suggest that Pakistan's current model is unsustainable. Without reforms, the system risks deepening the democratic deficit, weakening fundamental rights, and isolating Pakistan from global cybersecurity norms.

Cybersecurity Threats and Data Protection Gaps in Pakistan

We are living in the information age and the age of globalisation. Online utility bill payment, better medical infrastructure, modern transportation, usage of artificial intelligence, development of communication systems, technical warfare, and a plethora of other fields are all examples of the continuous expansion that modern states demonstrate. While technological advancements have shortened access, this has also given rise to new anxieties and risk factors. Hacking, information theft, money laundering, state secret acquisition, bank fraud, and threats to vital infrastructure are some of the cybercrimes that plague the digital world and are part of the ever-changing trends in cyber

warfare. Such dangers represent a problem for national security for both wealthy and emerging nations (Zahid, 2020). On the other hand, emerging nations with nuclear weapons, such as Pakistan, are more susceptible to these dangers. Another obstacle for Pakistan's government and lawmakers in their efforts to control the online space is the country's enormous population of internet users who lack basic IT skills (Zahid, 2020). Hackers in According to Sami, Pakistan have recently succeeded in penetrating the cyberspace of crucial installations and launched severe cyberattacks on crucial institutional websites. Pakistani lawmakers have passed cyber laws to forestall this, but these laws do not appear to address the full breadth and depth of the risks (Sami, 2024).

Automation, the cloud, big data, and artificial intelligence have all seen significant increases in usage over the last several decades, simplifying many aspects of human existence but also posing new dangers and complications. Data storage, privacy, security, and online crime are all impacted by these Internet problems. It is a daunting and deeply concerning task to deal with these new challenges, as technological advancements have sparked competition in cyberspace, leading to the emergence of proxy actors and organisations with political and ideological agendas (Hundley et al., 1995). Nowadays, cybersecurity is more important than ever before since computers are used in every aspect of life. Because of the occurrence of serious threats and the deficiency of effective formal procedures, internet security is of utmost importance for emerging nations in the third world. One example is Pakistan (Centre for Peace and Development Initiatives, 2020). There are a lot of reasons why the government has not fully executed its cybersecurity legislation, even though they were passed to control cyber risks and assaults (Privacy International, 2019). Furthermore, Pakistan's cyberspace has grown to 87 million broadband clients, with a diffusion rate of 39% over the past 20 years (PTA, 2020). Since the country has moved away from traditional infrastructure and towards digital systems, it is now susceptible to cyberattacks.

Legislative Challenges and the Need for Reform

In a report of 2019, Privacy International mentioned that issues about cybersecurity encompass the erroneous media portrayal of the subject, which predominantly presents the discourse from a

general standpoint, hence fostering a superficial understanding of cybersecurity among the public. Furthermore, there is an absence of an institutional framework to address this challenge, coupled with extensive security discussions regarding foreign threats that frequently overlook the cybersecurity challenges confronting the nation (Privacy International, 2019). The nation's conventional security culture, emphasising dangers such as border security, nuclear attack, and terrorism, encompasses the national security spectrum, therefore relegating cybersecurity to a secondary priority (Privacy International, 2019). The exclusion of the addressees in formulating the internet policy is a significant impediment since the absence of reaction from relevant stakeholders hinders progress mentioned by Privacy International in 2019.

However, the aforementioned cybersecurity law enacted in 2016 implemented several measures that were questioned due to the country's fragile democratic structure and were characterised as 'draconian' (Khan, 2016), a term not uncommon in underdeveloped nations such as Pakistan. Critics contend the law has conferred significant controls to the authorities, which are occasionally misused (Sridharan, 2016). It also lacks enough safeguards against the persistent threat of data breaches (Kalyar, 2020). The legislation fails to distinguish between cybercrime, cyber warfare, and cyber terrorism, resulting in inadequate and overly harsh sentences for the relevant offences (Aziz, 2018). Additionally, several observers characterise PECA as a governmental instrument employed to suppress dissenting voices under the guise of ‘national security’ and ‘anti-state’ language (Aziz, 2018). This sort of criticism and deficiencies also pertain to a significant problem in the creation and execution of cybersecurity measures. Pakistan, lacking support from corporate partners for the development of cybersecurity infrastructure, must consequently depend on internal investment (Baker, 2014). Two principal organisations are responsible for cybersecurity maintenance: the NR3C (National Response Centre for Cyber Crimes), operating below the FIA (principal law enforcement agency), and the Pakistan Information Security Association (PISA) (a nongovernmental entity), which collaborates with the private sector to address commercial-related issues (Baker, 2014).

The functioning of the state's cybersecurity is fundamentally deficient. The 2014 report *Cybersecurity in Pakistan: Regulations,*

Gaps and a Way Forward by Baker mentions that a practical, complete, and grassroots security policy appears to be absent, since the existing cybersecurity measures seem reactive, mostly aimed at 'extinguishing fires.' Furthermore, the existing cybersecurity measures are superficial, characterised by understaffed programs and mostly cosmetic interventions (Baker & Aamir, 2014). The methodology for addressing cybersecurity issues is 'security box-centric,' which throws out any type of 'out of the box solution,' placing excessive focus on the previous (Baker & Aamir, 2014). Problems with cybersecurity resolution are often the result of siloed thinking across several groups within an organisation, including but not limited to the risk, compliance, security, and IT audit divisions (Baker & Aamir, 2014). This discord is destructive as it leads to a squander of time and money (Baker & Aamir, 2014). Compounding this are the challenges associated with governance and excessive paperwork, wherein the majority of cybersecurity efforts and initiatives are predominantly theoretical, characterised by extensive policies and procedures. The *National Cyber Security Policy 2021* (Government of Pakistan, 2021) and subsequent analyses (Dawn, 2021) note that implementation is yet lacking a significant implementation strategy (typically only 5 to 10% of the sanctioned policy is executed in nearly all instances. Moreover, data theft constitutes a significant concern to the nation. The NADRA (National Database and Registration Authority) is the sole independent organisation in the country accountable for the government records and information of its people (World Bank, 2000). The susceptibility to data theft has escalated due to the linkage and dissemination of data to defence institutions and several government initiatives, like the Punjab Safe Cities Authority and the Benazir Income Support Program, among others (Kalyar, 2020). Two years ago, one of the greatest information breaches in Pakistan's history happened, compromising the data of millions of inhabitants of the PITB (Punjab Information Technology Board) (Kalyar, 2020).

According to *Foreign Affairs* (2020), there is no longer any room for discussion on whether authoritarian or democratic governments are more likely to utilise surveillance technology. To keep their populace under control, Saudi Arabia, China, and Russia are examples of tyrannical governments that use surveillance technology. Once people are aware that their conversations and

whereabouts are being observed, they alter their behaviour autonomously, which is why they believe surveillance technology to be successful Foreign Affairs, 2020). Democratic states, on the other hand, have the challenge of balancing state and citizen interests while using surveillance technology to enhance public safety and national security (Foreign Affairs, 2020). Thus, democratic regimes' exploitation of surveillance technology against their citizens is the primary focus of this study. Using surveillance technology to keep tabs on people goes against the very fabric of democratic governments' political culture, shattering long-held assumptions about what it means to be a democratic state (Foreign Affairs, 2020). In another report of 2020 titled *How technology strengthens autocracy*, Foreign Affairs put simply, the covenant between autonomous governments and their residents for guarantees of civil liberty and privacy is at odds with surveillance technology. Rapid technological advancement is widening the chasm between Democratic states and their citizens' understanding of their political culture; hence, immediate action is required to end this argument (Foreign Affairs, 2020). To better manage via social control, democratic regimes deploy monitoring technology (Monahan, 2018). Using monitoring ‘deliberately’ to promote societal goals of equality, justice, and fairness is what is meant by "democratic surveillance (Monahan, 2018). To paraphrase, theoretically, democratic regimes can maintain social control in check by instituting democratic controls, such as public accountability, openness, and citizen engagement (Monahan, 2018). Though they are often reactive and sluggish to react, democratic controls and public engagement can be successful in countering privacy-invasive monitoring in practice (Monahan, 2018). At the same time, democratic nations can now identify, follow, and analyse their inhabitants in real time, thanks to recent breakthroughs in surveillance technology (Zahid, 2020). So, left unregulated, digital mass monitoring has the potential to become the standard for democracies (Zahid, 2020). Tensions between political culture and surveillance technology are commonly seen in disagreements between legislators, security practitioners, and civil society members (Contestations of Internet Governance and Digital Authoritarianism in Pakistan, 2024).

Future Challenges

The capacity of states to conduct surveillance will expand dramatically due to two technological shifts: the adoption of 5G/6G networks and the integration of artificial intelligence (AI) into surveillance systems (Lin et al., 2021). The rollout of 5G and, eventually, 6G networks will enable ultrafast, low-latency communication between billions of devices (Lin et al., 2021). This interconnectivity, often described as the Internet of Things (IoT), will generate unprecedented volumes of personal data. Smart cities, autonomous vehicles, and sensor-driven infrastructure will produce continuous streams of location, behavioural, and biometric information (Lin et al., 2021). Without strong legal safeguards, this data can be subject to mass interception and profiling.

Tariq (2024) highlights the ethical and legal dilemmas surrounding algorithmic decision-making, particularly issues of accountability and transparency in AI systems. AI-powered analytics allow surveillance agencies to rapidly process and categorise vast datasets, including facial recognition, predictive policing, and real-time behavioural tracking. While such technologies can enhance national security and crime prevention, they also pose new risks of discrimination, lack of accountability, and opacity in decision-making. Issues of liability, such as responsibility for harm caused by algorithmic errors, further complicate regulatory frameworks (Tariq, 2024).

Pakistan currently lacks comprehensive legislation to address the implications of AI-enabled surveillance. Existing statutes such as PECA 2016 and IFTA 2013 do not account for predictive technologies, algorithmic bias, or the scale of data generated by IoT devices. This gap risks leaving individuals unprotected against future intrusions while granting unchecked power to state agencies.

Meeting these challenges requires proactive governance. Pakistan must anticipate how emerging technologies transform surveillance capability and embed safeguards such as mandatory algorithmic audits, transparency requirements, and liability rules before such technologies become entrenched. Lessons from the EU's GDPR and proposed AI Act illustrate how anticipatory regulation can strike a balance between innovation and rights protection (Abbasi, 2024).

In sum, Pakistan faces a critical juncture: as technology accelerates, the absence of forward-looking safeguards risks creating an environment where surveillance becomes normalised and accountability disappears.

Role of the State

To prevent the negative consequences of surveillance technology on democratic political culture, governments should participate in multilateral debates on an international level. There are two main reasons why nations will have a hard time agreeing on and implementing global norms and standards. For starters, geopolitical tensions stem from the fact that surveillance technologies have dual-use capabilities, serving both civilian and military purposes (Carnegie Endowment for International Peace, 2019). Since these technologies may boost both the economy and national defence, states are hesitant to limit their research and development of them (Carnegie Endowment for International Peace, 2019). Second, the pace of technology advancement is outpacing that of global governance (Centre for Peace and Development Initiatives, 2020). The Office of the Director of National Intelligence asserts that technological progress will persistently exceed the capacity of nations, agencies, and international organisations to establish standards, laws, regulations, and norms (Centre for Peace and Development Initiatives, 2020). The chasm between technological advancement and effective government will deepen in such a setting (Centre for Peace and Development Initiatives, 2020). However, further avenues for international cooperation exist for the advancement of human rights, ethical principles, and safety standards. Numerous worldwide organisations, including the ICRC (International Committee of the Red Cross) and NATO (North Atlantic Treaty Organisation), present balances to find common principles and methods for enhancing monitoring systems (ICRC, 2024; NATO, 2021). Also, the OECD Principles on AI do not have any legal force, but they do lay out a political will to advance AI that is reliable, considerate of human rights, and upholds democratic principles (North Atlantic Treaty Organisation, 1949). Furthermore, the World Economic Forum spearheads a project to convene public and private sector players to formulate and evaluate policy frameworks about artificial

intelligence, machine learning, and face recognition systems (World Economic Forum, 2023). Achieving international collaboration begins with such endeavours. On the domestic front, governments should discuss monitoring technology with their residents and consider passing thorough privacy and security regulations. To begin, it is widely believed that the General Data Protection Regulation (GDPR) of the European Union is among the most stringent and all-encompassing privacy and security regulations in the world (European Union, 2016). When the GDPR was enacted in 2016, surveillance technology was far behind what it is now. So, critics are demanding changes to that regulation because, by limiting data gathering and sharing, they impede AI research and usage (European Union, 2016). While the regulation does place restrictions on real-time face recognition by requiring users' permission, it does so with some caveats, including for usage by law enforcement, for private purposes, and in case where an individual cannot be positively recognised. Thus, although the regulation provides a solid foundation upon which to construct an all-encompassing privacy and security regulation, it would be wise to broaden its scope to incorporate new technology and the effects it may have on both (European Union, 2016).

Results

Applying the evaluation rubric of necessity, proportionality, legality, oversight, and remedies to Pakistan's surveillance regime reveals several key findings:

1. **Necessity**
   The IFTA 2013 and PECA 2016 were enacted with the stated purpose of countering terrorism and cybercrime. However, neither law clearly defines the scope of "necessity." Instead, both provide broad powers to law enforcement agencies without requiring evidence that less intrusive means were considered.

2. **Proportionality**
   The scope of surveillance authorised under IFTA allows interception of communications for wide categories of "scheduled offences." Judicial oversight is limited to ex parte applications, with little transparency. PECA's Section

20 (criminalisation of defamation) has been disproportionately applied against journalists and activists, illustrating how surveillance-linked provisions restrict free expression (Dawn, 2024b).

3. **Legality**
   While the Constitution guarantees privacy under Article 14, statutory language in s.54 of the Pakistan Telecommunication Act 1996 authorises executive monitoring on grounds of "national security" without defining the term. This vagueness undermines the principle of legality under international human rights law.

4. **Oversight**
   Pakistan lacks independent oversight bodies comparable to data protection authorities in the EU. Requests for surveillance under IFTA are not accompanied by published reporting, nor are there mechanisms for parliamentary or civilian review.

5. **Remedies**
   There are no explicit statutory remedies for individuals whose rights are violated by unlawful surveillance. Judicial recourse exists in principle, but litigation is costly and protracted, making effective redress inaccessible.

Overall finding: Pakistan's surveillance laws provide a legal basis for state monitoring but fail to satisfy international standards of necessity, proportionality, legality, independent oversight, and effective remedies.

Recommendations

This study proposes a set of reforms that are staged, specific, and testable.

The first recommendation is to amend problematic PECA provisions. This includes repealing or narrowing Section 20, which criminalises defamation and has been used to silence journalists and political opposition. It also involves inserting safeguards to ensure that speech restrictions are strictly limited to incitement of violence or hate speech, in line with ICCPR standards.

The second recommendation focuses on codifying warrant and oversight procedures under IFTA. It requires prior judicial authorisation for all forms of electronic surveillance and mandates that warrants specify the target, scope, duration, and justification of surveillance. Additionally, it establishes a right of post-surveillance notice to affected individuals, with exceptions only for narrowly defined national security cases.

The third recommendation emphasises independent oversight and transparency. This involves establishing a National Cyber Coordination Centre (NCCC) with defined civilian oversight, requiring annual transparency reports detailing the number, type, and outcome of surveillance authorisations, and introducing parliamentary scrutiny of the NCCC's activities.

The fourth recommendation aims to strengthen remedies. It proposes providing statutory rights of appeal and compensation for unlawful surveillance and creating a specialised ombudsman or tribunal for citizens to seek redress.

The fifth recommendation focuses on integrating AI and emerging technologies into governance. It suggests developing a National AI Strategy that addresses privacy, accountability, and security risks associated with algorithmic surveillance. It also recommends forming a Privacy and Security Task Force with members from government, academia, and civil society, tasked with producing deliverables such as draft legislation, annual risk assessments, and AI ethics guidelines within fixed timelines.

The sixth recommendation concerns international cooperation. It advises aligning Pakistan's framework with the ICCPR, GDPR, and the Necessary & Proportionate Principles, and entering into regional and international agreements to share best practices while ensuring that domestic safeguards remain intact.

Collectively, these staged reforms ensure that Pakistan's surveillance framework protects fundamental rights while maintaining operational capacity for genuine security threats.

Conclusion

This study has shown that while Pakistan constitutionally guarantees the right to privacy under Article 14, its statutory and institutional framework for surveillance falls short of international human rights standards. The analysis of IFTA 2013, PECA 2016,

and s.54 of the Pakistan Telecommunication Act, 1996 demonstrates that existing laws provide wide discretion to state agencies without sufficient safeguards of necessity, proportionality, or legality. The absence of independent oversight and effective remedies further deepens the risk of abuse.

These shortcomings have direct implications for democratic governance. When surveillance is conducted without transparency and judicial control, it undermines civil liberties, weakens public trust, and risks the politicisation of law enforcement. Comparative experience, particularly under the ICCPR, the Necessary & Proportionate Principles, and the GDPR, illustrates that effective security can be achieved without sacrificing fundamental rights.

Looking forward, Pakistan stands at a critical juncture. The rapid expansion of 5G, IoT, and AI technologies will intensify surveillance capacities, making the need for reform more urgent. Implementing codified warrant standards, establishing independent oversight, introducing post-surveillance remedies, and adopting a proactive AI governance strategy will be essential steps.

In sum, Pakistan's challenge is not whether to regulate surveillance, but how to do so in a way that reconciles national security with the protection of fundamental rights. A forward-looking, rights-based surveillance framework will not only strengthen democratic accountability at home but also align Pakistan with global cybersecurity and human rights norms.

References

Abbasi, S. (2024, October 22). *Caught in the web: Surveillance, data protection and AI in Pakistan*. *Dawn*.

Aftab, S. (2024). *Comparative Perspectives on the Right to Privacy: Pakistani and European Experiences*. Springer Nature

Akhter Hamid Ghori v. Saima Estate Developers, 1989 CLC 2173 (Pakistan).

Alam, M. Z., & Warraich, G. I. (2024). *A Comparative Analysis of Legal Framework for Data Protection in Global Jurisdictions*. Pakistan Journal of International Affairs, 7(3)

Amicelle, A. (2022). *Big data surveillance across fields: Algorithmic governance for policing and regulation*. Big Data & Society, 9(2)

Andrejevic, M. (2014). *Surveillance in the Big Data era. In K. D. Pimple (Ed.),* Emerging pervasive information and York: Springer.

Baker, S., & Aamir, M. (2014). *Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward*. Society, Law and Policy Review,

Brennan Center for Justice. (2019, July 10). *Map: Social media monitoring by police departments, cities, and counties.* https://www.brennancenter.org/ourwork/researchreports/mapsocialmediamonitoringpolicedepartmentscitiesandcounties

Benazir Bhutto v. Federation of Pakistan, PLD 1998 SC 388 (Supreme Court of Pakistan).

Carnegie Endowment for International Peace. (2019, September 17). *The global expansion of AI surveillance.* https://carnegieendowment.org/research/2019/09/theglobalexpansionofaisurveillance?lang=en

Centre for Peace and Development Initiatives. (2020, June 10). *Status of right to information (RTI) in Pakistan 2020*. http://www.cpdipakistan.org/wpcontent/uploads/2020/09/StatusofRTIinPakistan2020.pdf

Contestations of internet governance and digital authoritarianism in Pakistan. (2024). *International Journal of Politics, Culture, and Society.*

Cukier, K. (2021, March 9). *Surveillance is a fact of life, so make privacy a human right*. The Economist.

Daily Times. (2024). *Prevention of Electronic Crimes Act (PECA) – Pakistan's cybercrime legislation: Impact, concerns & implementation*. Daily Times.

Dawn. (2021, July 28). *Pakistan approves first-ever National Cyber Security Policy*. Dawn. https://www.dawn.com/news/1637409

Dawn. (2024a, December 14). *Journalists, vloggers among 150 booked under PECA*. Dawn.

Dawn. (2024b, December 15). *PFUJ condemns arrest orders against journalists under PECA*. Dawn.

Digital Rights Foundation. (2020). *Impact and Legality of Surveillance: The Investigation for Fair Trial Act, 2013*. Digital Rights Foundation.

European Commission. (2019, April). *Ethics guidelines for trustworthy AI.* https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

European Data Protection Board. (2019, July 10). *Guidelines 3/2019 on processing of personal data through video devices*. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Federal Investigation Agency Act, 1974, s 5. (1974).

Feldstein, S. (2019, September 17). *The global expansion of AI surveillance.* Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/globalexpansionofaisurveillancepub79847

Foreign Affairs. (2020). *The digital dictators: How technology strengthens autocracy* (Vol. 2). https://www.foreignaffairs.com/articles/china/20200206/digitaldictators

Foreign Affairs. (2020, February 6). *How technology strengthens autocracy*. *Foreign Affairs*.

Government of Pakistan. (2021). *National Cyber Security Policy 2021*. Ministry of Information Technology & Telecommunication, Islamabad. Retrieved from https://scci.com.pk/jotelab/2023/02/National-Cyber-Security-Policy-2021-Final-1.pdf

Heilweil, R. (2020, May 8). *The world's scariest facial recognition company, explained*. Vox. https://www.vox.com/recode/2020/2/11/21131991/clearviewaifacialrecognitiondatabaselawenforcement

Hill, K. (2020, January 18). *The secretive company that might end privacy as we know it*. The New York Times. https://www.nytimes.com/2020/01/18/technology/clearviewprivacyfacialrecognition.html

ICRC President. (2024, June 1). *"We must adopt a human-centered approach to the development and use of new technologies" [Speech at Shangri-La Dialogue, Singapore]*. International Committee of the Red Cross (ICRC). https://www.icrc.org/en/statement/icrc-president-we-must-adopt-human-centered-approach-development-and-use-new-technologies

International Journal of Research in Humanities and Social Studies. (2015). *National security: Concepts and definitions*. IJRHSS, 2(1), 11–18. Retrieved from https://www.ijrhss.org/pdf/v1-i2/2.pdf

Kalyar, J. A. (2020, March 2). *Pakistan's cybersecurity regime*.

Kendall Taylor, A., Franz, E., & Wright, J. (2020*). The digital dictators: How technology strengthens autocracy*. Foreign Affairs, 99(2), 103. https://www.foreignaffairs.com/articles/china/20200206/digitaldictators

Lin, X., Chen, M., Rydén, H., Jeong, J., Lee, H., Sundberg, M., Timo, R., Razaghi, H. S., & Poor, H. V. (2021). *Fueling the next quantum leap in cellular networks: Embracing AI in 5G evolution towards 6G. IEEE Communications Magazine*, *59*(12), 76–82. https://doi.org/10.1109/MCOM.001.2100373

Monahan, T. (2017). Regulating belonging: Surveillance, inequality, and the cultural production of abjection. *Journal of Cultural Economy*, *10*(2), 191–206. https://doi.org/10.1080/17530350.2016.1150588

Monahan, T. (2018). Ways of being seen: Surveillance art and the interpellation of viewing subjects. *Cultural Studies*, *32*(4), 560–581. https://doi.org/10.1080/09502386.2018.1450634

NATO. (2021, October 4). *Critical infrastructure protection & resilience — NATO sets a standard for ethical use of new technologies*. *European Commission Newsroom.* https://ec.europa.eu/newsroom

Necessary & Proportionate. (2014, May). *International principles on the application of human rights to communications surveillance*. https://www.ohchr.org/documents/issues/privacy/electronicfrontierfoundation.pdf

Pakistan Telecommunication (Reorganisation) Act, 1996, s 54. (1996).

Pakistan Telecommunications Authority. (2024). *Annual report: 2024.* *https://www.pta.gov.pk/assets/media/pta_ann_rep_2024_27032020.pdf*

Privacy International. (2019, February). *Guide to international law and surveillance 2.0*. https://privacyinternational.org/sites/default/files/201904/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf

Richards, N. M. (2013). *The dangers of surveillance*. Harvard Law Review, 126, 1935.

https://harvardlawreview.org/wpcontent/uploads/pdfs/vol126_richards.pdf

Sami, W. (2024, September 19). *Pakistan's cybersecurity challenges: A complex digital landscape.* STRAFASIA. https://strafasia.com/pakistanscybersecuritychallengesacomplexdigital

Sayyed, S., & Aamir, M. (2021). *Cybersecurity in Pakistan: Regulations, Gaps and Way Forward*. IIU Law Review, 1(3).

Tariq, Ayesha. (2024). *Artificial Intelligence and the Law: Ethical and Legal Dilemmas in Algorithmic Decision-Making*. *Fari Journal of Social Sciences and Law*,

The National Assembly of Pakistan. (1973, March 14). *Debates, official report: Constitution making*. http://na.gov.pk/uploads/documents/1453439967_808.pdf

The News. (2018, December 19). *In Pakistan, banking sector most vulnerable to cyber-attacks*. The News International.

United Nations General Assembly. (1948). *Universal Declaration of Human Rights* (UNGA Res 217 A (III)). https://treaties.un.org/doc/publication/unts/volume%20999/volume999i14668english.pdf

United Nations Human Rights Committee. (1988). *General comment No. 16: Article 17 (Right to privacy) – The right to respect of privacy, family, home and correspondence, and protection of honour and reputation*. U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I), p. 142.

United Nations Human Rights Council. (2019, May 28). *Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/41/35). https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session41/Pages/ListReports.aspx

United Nations. (1966). *International Covenant on Civil and Political Rights* (999 UNTS 171). Adopted 16 December 1966, entered into force 23 March 1976. https://treaties.un.org/doc/publication/unts/volume%20999/volume999i14668english.pdf

United Nations. (1989). *United Nations Convention on the Rights of the Child* (1577 UNTS 3). Adopted 20 November 1989, entered into force 2 September 1990. https://treaties.un.org/doc/publication/unts/volume%20999/volume999i14668english.pdf

Waqar, M., & Khan, U. (2020). *Cybersecurity in Pakistan: Regulations, Gaps and Way Forward*. PJCL,

World Bank. (2000). *Project document: NADRA's institutional establishment*. World Bank / Government of Pakistan.

World Economic Forum. (2023, June 15). *World Economic Forum launches AI Governance Alliance focused on Responsible Generative AI*

World Economic Forum. (n.d.). *Shaping the future of technology governance: Artificial intelligence and machine learning*. Retrieved April 1, 2020, from https://www.weforum.org/platforms/shapingthefutureoftechnologygovernanceartificialintelligenceandmachinelearning/

Zahid, L. (2020, February 6). *In dire straits: Pakistan's web monitoring.* MIT Technology Review. http://www.technologyreview.pk/indirestraitspakistanswebmonitoring/