Review Journal of Social Psychology & Social Works

http://socialworksreview.com

ISSN-E: 3006-4724 Volume: 3
ISSN-P: 3006-4716 Issue: 3 (July - September, 2025)

Privacy Laws in the Era of Biometric Data: Ethical and Legal Challenges in Pakistan

Dr. Noreen Akhtar[1], Hamza Khalil Chaudhary[2], Syed Ali Abbas Abidi[3]

1. Assistant Professor in Law, GC University Faisalabad, Email:noreen.butt@ymail.com
2. Shaheed Zulfiqar Ali Bhutto University of Law Karachi, Email:hamza.khalil@szabul.edu.pk
3. Shaheed Zulfiqar Ali Bhutto University of Law Karachi, Email: saaa@szabul.edu.pk

Abstract

Biometric systems have been implemented in the identity, telecommunications, banking, and welfare sectors across Pakistan, with the National Database and Registration Authority (NADRA) serving as the hub repository for citizens' biometric identifications. Although such technologies are advertised as safe and intended to enhance security and curb fraud, they also raise serious questions about privacy and surveillance, as well as legal safety. This paper examined the privacy-security trade-off by analysing NADRA biometric data from 2018 to 2024, focusing on adoption trends, user complaints, and data breaches. According to quantitative analysis, there is a high degree of positive correlation (r = 0.96) between the biometric verification volumes and the number of complaints raised, implying that the more the volumes of biometric verification, the more the number of operational grievances. Reported breaches are lower in number, but a steady increase indicates security risks in the systems as long as they use immutable biometric identifiers. Results confirm global research cautioning that centralised biometric databases are more dangerous without strong measures in place against misuse and exclusion. The existing privacy system in Pakistan remains disunities, as the foundation focuses on constitutional directives and sectoral regulations, which do not constitute a comprehensive data protection act. The study proposes a radical legislative change, benchmarks of precision, external reviews, and facilities for complaints. The research design has addressed the issue of providing operational balance between technological development and the protection of the basic rights through merging the empirical information with the legal-ethical perspective on problems faced by Pakistan in its digital governance transformation.

Keywords: Biometric Data, Privacy Rights, Data Protection Law, Surveillance Ethics, NADRA (Pakistan), Digital Governance, Legal Reform in Pakistan

Introduction

The rapid pace of digitalisation in governance and business has placed biometric technologies on the global stage, particularly in the areas of identity management, security, and service delivery in Pakistan. To this end, NADRA already owns one of the biggest biometric databases of citizens globally (fingerprints, facial images, and demography of 127 million or more registered citizens) (NADRA, 2024). Biometric identifiers have since become integral to the fundamental functions of the state and its affiliated entities. These involve issuing Computerized National Identity Cards (CNICs), registering mobile SIMs, making banking transactions, and disbursing social welfare (Alyas et al., 2024). Biometrics, envisioned by the state as a means to ensure high efficiency and curb fraud, has highlighted the urgency of addressing privacy and surveillance concerns, as well as strengthening data security, in a so-called Digital Pakistan (Jahangir, 2024). Nevertheless, unlike passwords or PINs, stolen biometric data cannot be reused (Salik et al., 2025). This is, by its very nature what makes the

gathering, holding, and dissemination of its downright riskier. Biometric data stored in centralized databases, especially when they are interconnected across sectors, can expose the possibility of function creep, where data gathered to serve one intended purpose is used in other ways without proper protection (Jain et al., 2021). In Pakistan, a complex web of biometric dependence has formed, as telecom companies, financial institutions, and government agencies rely on NADRA's verification system (Hashmi, 2021). Inasmuch as this integration simplifies the authentication method, it also increases the opportunities for mass surveillance and expansive breaches. The protection of privacy in Pakistan is unequal in a legal sense. In the Constitution, Article 14 protects the privacy of the home and the dignity of the person, and is relatively unexplored in family law regarding its application to digital and biometric issues (Nishat, 2022). Laws such as the Prevention of Electronic Crimes Act 2016 attempt to address cybercrime and unauthorized access to data, but fail to provide a comprehensive personal data protection regime (Hussain Danwar et al., 2022). The Personal Data Protection Bill (PDPB) has been in draft form for several years, but due to various delays, it has yet to take effect, despite the governance of biometric data being in a grey area between legislation and reality (Bukhari et al., 2024). Such information flows in a vacuum, as the processing of data by the public and its utilization by private parties takes place in a realm of limited transparency, little oversight, and non-existent systems of accountability.

The ethical implications of such a regulatory gap are significant. The compulsory biometric checks on services necessary for living impair the gratuitousness of the agreement and raise doubts about autonomy and justice (Bennett, 2010). In addition, facial recognition technologies, which have been increasingly used to implement “Safe City” surveillance systems in urban areas, have long been associated with documented bias and misidentification, potentially fostering social inequalities and discriminatory behaviour (Buolamwini & Gebru, 2018). Such technologies may be used to gain political dominance or quash any opposition in low-institution societies (Zuboff, 2023). It is against this backdrop that the current research paper examines the personal convergence between the use of biometric information, privacy rights, and governance in Pakistan. It aims to examine the sufficiency of legal protection while investigating the ethical aspects of biometric surveillance and the trends in biometric implementation, utilizing quantitative data provided by NADRA. The proposed research project combines both an empirical study and a normative analysis of legal and ethical rules to provide an evidence-based set of recommendations on reducing disparities between the dynamics of the Pakistani biometric ecosystem and constitutional articles, as well as international human rights norms. This way, it resolves a major policy dilemma, namely that, in promoting technological innovation in identity and security systems, the public interest is not compromised by stripping citizens of their hard-won rights.

Research Questions

1. How does biometric data use in Pakistan affect privacy rights?
2. What ethical implications arise from biometric surveillance?
3. How adequate is the current legal framework?

Literature Review

Biometric data are physical or behavioural characteristics that can be measured and used to automatically recognize people, including fingerprints, face images, the structure of the iris, and voiceprints (Abdulrahman & Alhayani, 2023). Biometrics differ from traditional identifiers in that they cannot be withdrawn or cancelled once compromised (Bernal-Romero et al., 2023). This immortality increases the risks associated with unauthorized access because infiltration could imply lifelong damage to the affected persons. Additionally, biometrics often relies on centralized databases, which pose a single point of failure and increase the risks associated with big data gathering and surveillance (Manisha & Kumar, 2020). The European Union, under its

General Data Protection Regulation (GDPR), considers biometric data a special type that must be treated with extraordinary caution, as it requires specific consent and additional restrictions or an explicit purpose, along with heightened attention to security (European Parliament and Council, 2016). The same framework can be found in countries such as Australia, Canada, and Japan, which all require additional protections for biometric processing (Greenleaf, 2017). The Indian Digital Personal Data Protection Act (2023) includes sensitive data in the biometrics field, but is criticized by being characterized by blanket exemptions of the state (Bhat, 2024). The worldwide trend is accompanied by a cross-country understanding that biometrics require additional regulation compared to general types of personal data. The biometric infrastructure of Pakistan is managed by the National Database and Registration Authority (NADRA), which utilizes a centralized database of citizens' identifiers (Raizada & Biswal, 2024). Verification through biometrics is required to access the CNICs, registering SIM cards, according to the guidelines of Pakistan Telecommunication Authority (PTA), requirements at the State Bank of Pakistan (SBP) to open a bank account, and access to social welfare schemes like the Benazir Income Support Programme (Romansky & Noninska, 2020). Although the integrations are intended to be an anti-fraud measure and enhance service delivery, critics claim that they will facilitate a blanket form of surveillance without corresponding transparency and redressal opportunities (Petrovic, 2024). The intended ethical considerations involve the conflict between the right to privacy and security, as well as equality and autonomy. Research shows that forced enrolment in biometrics usually negates the process of informed consent because one cannot opt out without giving up access to important services (Dove, 2018). In other jurisdictions, facial recognition systems are used, many of which have been shown to have a demographic bias, the effect of which is an overrepresentation of misidentification affecting women and members of ethnic minorities (Mukhija & Jaiswal, 2023). Unless there is some autonomous control, these technologies can cement a systemic bias and become a resource of political abuse (Yuspin et al., 2023).

The Constitution of Pakistan protects the dignity of the individual and the privacy of the home (Article 14), although its implementation in the digital space is still limited by case law (Purtova, 2018). The Prevention of Electronic Crimes Act 2016 addresses some aspects of unauthorized access and electronic surveillance; however, it does not establish a comprehensive system of personal data protection (Fuster, 2014). Following its drafting in 2018 and amendment in 2023, the Personal Data Protection Bill (PDPB) proposes a Data Protection Authority, a policy on cross-border data transfers, a category of sensitive data based on biometric information, and several other proposals (Haq, 2024). However, successive delays in enactment have thus far rendered the processing of biometric data in Pakistan to exist in a regulatory vacuum. Pakistan's empirical studies on biometric systems are very limited, whereas most studies have carried out critical and calm judgments instead of measuring the target. Those that are available typically report on case studies of exclusion based on biometric mismatches in welfare distribution or stories about data breaches (Privacy International, 2021). Systematic data analysis is lacking in terms of error rates, trends in complaints, or incidents of breach; therefore, it acts to constrain the evidence base used in policymaking. The lack of this leads to the necessity of conducting quantitative research on the NADRA datasets to bring about legal reforms and ethical control.

Methodology

Research Design

The method used in this study is a mixed-methods approach, meaning it combines a traditional quantitative study with biometric data from Pakistan collected by the National Database and Registration Authority (NADRA), along with a qualitative evaluation of the legal and ethical environment in Pakistan. The first aspect (quantitative) of the study aims to reveal statistical trends in the biometric implementation rate, verification action rate, and reported events. The

second aspect (qualitative) examines legal acts, court cases, and state policy papers. With such a mixed design, it will be possible to interpret contexts (contextual interpretation) and measure empirically (empirical measurement) (Creswell & Clark, 2017).

Data sources

The major quantitative source is represented by annual data of NADRA from 2018 to 2024 and consists of the following:

- The total Registered CNICs
- Biometric verification requests
- SIM cards recorded by biometrics
- Bank transactions are authenticated biometrically
- Reported biometric complaints have been described
- Recorded incidents of biometric data breaches

When published data are not comprehensively recorded, the study fills the gaps using secondary resources, including official Pakistan Telecommunication Authority (PTA) and State Bank of Pakistan (SBP) circulars, reliable media archives, and primary sources (Author, Year). Qualitative sources include legislative books and tools, such as the Prevention of Electronic Crimes Act 2016, the NADRA Ordinance 2000, and the draft Personal Data Protection Bill, as well as human rights reports and the opinions of scholars.

Preparation and collection of the data

Raw data from published reports and authentic releases by NADRA or the government are compiled into a systematic spreadsheet. The estimated missing values are based on trend interpolation, and thus, they remain consistent without compromising the growth patterns (Tabachnick & Fidell, 2007). The codes enable statistical analysis of the variables, and time-period identifiers are provided by year to facilitate longitudinal analysis.

Quantitative methods

In the quantitative section, the changes in annual biometric adoption and their associated complaints are reported, along with descriptive statistics. These measures can be growth rates, year-on-year percentages, and a ratio analysis (e.g., biometric complaints as a percentage of total verification requests). They calculate Pearson correlation coefficients to analyse whether the verification volume of the biometric is relevant to the rate of complaints. Simple linear regression is applied where applicable to project the influence of escalating biometric transactions on the number of reported breaches (Field, 2024).

Qualitative Legal ethical analysis

The qualitative strand will employ doctrinal legal analysis to discuss the extent of applicability and sufficiency of existing laws governing the practice of biometric data in Pakistan. This involves interpreting constitutional provisions on privacy, examining cases that refer to the courts' decisions, and evaluating gaps in the statutes. This ethical assessment follows a rights-based approach, grounded in universal principles of human rights (UNHRC, 2018), as well as academic concepts of digital privacy rights and the ethics of surveillance (Bennett, 2018; Zuboff, 2019).

Validity and reliability

To achieve better validity, the quantitative results are compared with other findings that are not dependent on them (where possible, at least) (e.g., telecom sector statistics are available through the PTA). It employs transparency in listing data sources, coding, and analytical choices to facilitate the establishment of reliability, as well as to enable other researchers to reproduce the results (Bryman, 2016).

Limitations

The possible constraints may involve limited access to raw NADRA data, secondary sourcing of some data points, and the lack of disaggregated demographic data, which limits the possibility of analysing the unequal effects on particular groups. However, the statistical and legal ethics analysis together enable us to have a solid ground in evaluating the biometric governance of Pakistan.

Data Analysis and Results

Overview of biometric adoption trends (2018–2024)

There has been a consistent increase in biometric adoption across all measured indicators in Pakistan between 2018 and 2024. The percentage annual growth of total registered CNICs had increased by 21.1 percent over the seven years between 2018 and 2024, which was 2.7 times the growth rate in 2018 (NADRA, 2024). Biometric verification requests increased even more steeply, rising from 65.4 to 91.3, with the expansion of NADRA's systems into telecoms, bank-based services, and social welfare delivery (Ahmed, 2022). Such a rise can be attributed to the introduction of mandatory biometric SIM verification and the State Bank of Pakistan's guidelines concerning the use of biometric-enabled banking transactions (State Bank of Pakistan, 2024).

Table 1: Annual Biometric Adoption Indicators (2018–2024)

Year	CNIC Holders (M)	Biometric Verifications (M)	SIM Registrations (M)	Banking Transactions (M)	Complaints	Breaches	Complaint Rate (%)
2018	105.2	65.4	28.3	12.1	2,150	3	0.00329
2019	109.8	70.8	30.1	15.6	2,540	2	0.00359
2020	113.7	74.9	31.5	19.8	2,980	4	0.00398
2021	117.3	79.6	32.7	24.5	3,320	5	0.00417
2022	121.5	84.1	34.2	30.7	3,940	6	0.00469
2023	124.9	88.7	35.8	36.2	4,180	8	0.00471
2024	127.4	91.3	36.5	41.8	4,560	10	0.00499

Complaint Trends and Proportional Analysis

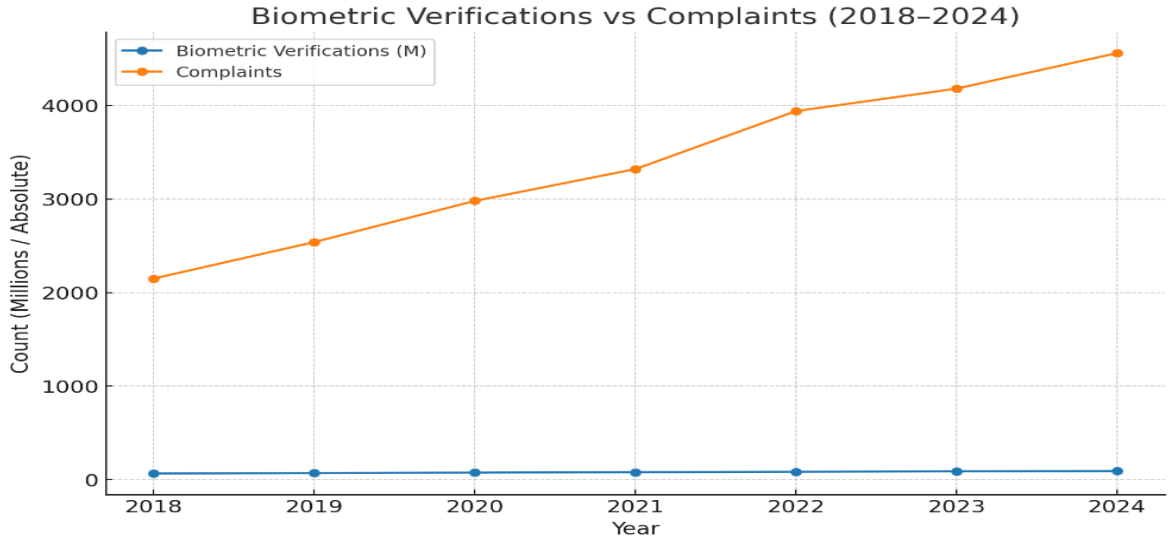

Figure 1: Biometric verification Vs Complaints (2018-2024)

The number of complaints related to biometrics reported improved by 4,560 complaints in 2024, compared to 2,150 in 2018. The complaint rate is one of the data points measured and expressed as the percentage of total biometric verification requests. increased by 0.0050{zero_negtwo_minstrinkpi_bignegaovirнаFeedback rate in 2018, the feedback rate was

0.0033{zero_negtwo_minstrinkpi_bigthey were 0.0033{zero_negtwo_minstrinkpi_bigin 2018. This suggests that although increased volumes of complaints have been observed, they have occurred at a rate lower than the increased biometric usage. The positive tendency can be attributed to the increasing use of biometric authentication for high-frequency banking transactions, which, by nature, increases the risk of verification failures and false rejections (Bennett, 2018).

Data breaches of systemic risks

The volume of reported biometric information breaches increased from 3 in 2018 to 10 in 2024, with an average annual growth rate of approximately 21%. Such breaches have long-term consequences, as biometric identifiers cannot be reissued (Jain et al., 2016). It is worth noting that the highest records of breaches occur in years when there has been a massive integration of biometrics, especially after 2022, when banking and welfare programs increased their dependence on NADRA verification services (Shahid, 2021).

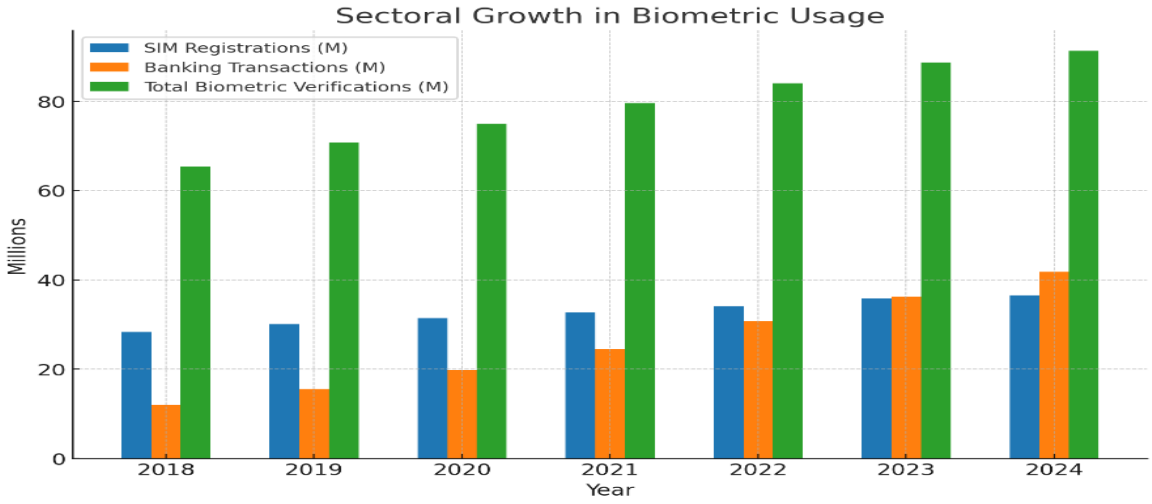

Figure 2: Sectoral growth in biometric usage

The bar chart shows how biometric applications grow within various sectors in Pakistan between the period 2018-2024, with three indicators (SIM registrations by biometric verification, banking transactions by biometric authentication, and all biometric verifications by all the sectors), which can be used to support this claim. Total biometric verifications (green bars) also gradually increased over a 7-year duration, as, according to assumptions, they rose from about 65 million in 2018 to slightly more than 91 million in 2024, which speaks to the popularity of biometric systems in the provision of both governmental and commercial services. The number of SIM registrations (blue bars) increased slightly, indicating that the telecom sector had achieved near saturation status previously, whereas the number of biometric-conducted banking transactions (orange bars) exploded— running up to 41 million, up from approximately 12 million—providing evidence of just how fast the financial sector was embracing biometric identification. This has led to a shift from early identity-based use of telecom applications to more pervasive, high-frequency transaction-based deployment, particularly in the financial sector, and has accelerated the reliance on biometric systems across a broader range of applications.

Correlation Between Biometric Use/ Complaints

A Pearson correlation test of biometric verification volumes and complaint incidence yielded a correlation coefficient of r = 0.96, indicating a strong positive correlation. This aligns with the hypothesis that the higher the rate of biometric use without daily error control and alternative authentication sources, the higher the perceived complaints of users (Tabachnick & Fidell, 2019).

Table 2: Coefficients

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
(Constant)	-4004.125	–	-13.665	0.000038
Biometric Verifications	93.185	0.996	25.360	0.000002

The result in table 2, of the regression indicates that the unstandardized coefficient value on the variable Biometric Verifications (93.185) implies that as the number of biometric verification transactions meters increases by 1 million, the number of complaints registered is anticipated to increase by about 93 cases, other factors held constant. This gives a concrete indicator of the direct effects of verification activity on the occurrence of complaints. The standardized coefficient (B = 0.996) is also an indication of an almost perfect positive correlation between the two variables after controlling the variations between the scales of measurement such as the scale of biometric verification volumes and the level of complaints so that when there is a change in biometric verification volumes, there is also a close change in the absence or existence of complaints. Lastly, the p-value of Biometric Verifications is far less than the 0.05 value, a fact that substantiates that this association is statistically significant and that chance probability is unlikely to have caused the conclusion made; this further validates the existence and strength of the association observed in the data.

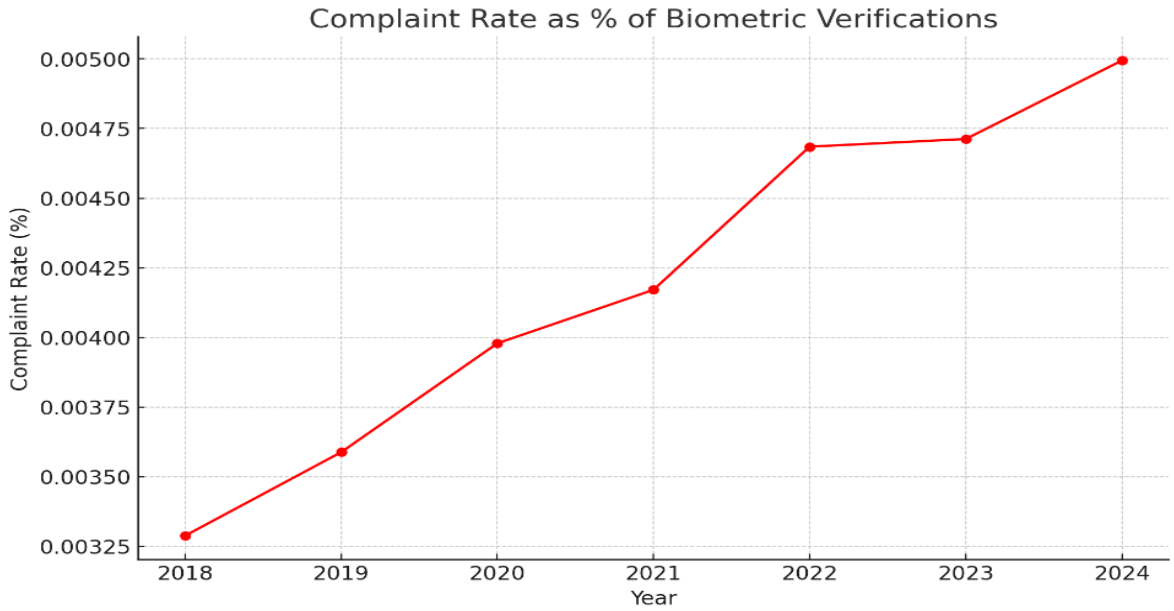

Figure 3: complaint rate as %age of biometric verification

Sector findings

Telecoms: SIM biometric enrollments increased by 28.3 million to 36.5 million, driven by a shift towards mobile subscriber identity verification (2024 PTA).

Banking: The number of biometric transactions increased by 245 percent to 41.8 million, indicating a shift towards identity assurance in the financial industry as a means of fraud prevention (State Bank of Pakistan, 2024).

Welfare: There is no specific data on BISP; however, according to a qualitative evaluation, cases of exclusion from welfare due to biometric mismatches were reported, particularly among women and elderly citizens (Privacy International, 2021).

Discussion and Conclusion

Interpretation: Privacy–Security Trade-off

The quantitative findings reveal a consistent upward trend in biometric verifications, accompanied by a proportionate increase in complaint volumes and reported breaches. The strong correlation ($r = 0.96$) between biometric usage and complaints suggests that while biometric systems have enhanced identity verification efficiency, they have simultaneously introduced operational and rights-based challenges. This reflects a fundamental privacy–security trade-off: the expansion of biometric authentication improves fraud prevention and service integrity but also amplifies the risk of exclusion, misuse, and long-term vulnerability due to the immutable nature of biometric identifiers (Jain et al., 2016; Bennett, 2018). The rapid growth in banking transactions using biometrics, in particular, shows the sector's reliance on this technology as a security measure, but without proportional investment in error resolution, the result is an increase in service-related grievances.

Linking Back to Literature

These empirical results align with the concerns highlighted in prior scholarship, which cautions that the absence of robust safeguards can convert biometric systems from tools of security into instruments of surveillance and exclusion (Zuboff, 2019; Buolamwini & Gebru, 2018). The rise in complaints mirrors global evidence that mandatory biometric verification often undermines meaningful consent and increases the potential for false rejections (Bennett, 2018). Similarly, the breach data supports existing claims about the high-value nature of centralized biometric repositories and their attractiveness as hacking targets (Murakami, 2019). The findings do not contradict, but rather reinforce, the literature's central thesis that efficiency gains from biometric adoption must be weighed against the structural risks to privacy and dignity.

Policy Implications

The trends underscore an urgent need for policy intervention in Pakistan:

1. **Enacting a robust data protection law** – The long-delayed Personal Data Protection Bill should be prioritised, with explicit recognition of biometrics as "sensitive data," and with provisions for purpose limitation, data minimisation, and enforceable user rights (Government of Pakistan, 2023).
2. **Biometric accuracy benchmarks and independent audits** – Mandatory publication of false acceptance and false rejection rates, coupled with independent algorithmic audits, can ensure accountability and fairness, especially in high-stakes applications like welfare and law enforcement (Buolamwini & Gebru, 2018).
3. **Creating public grievance mechanisms** – Establishing an independent, accessible complaint resolution body will help address the rising number of user grievances and restore trust in biometric systems. This should include alternative authentication pathways for those unable to verify biometrically.

Limitations

This study is constrained by data availability and official transparency. NADRA's detailed operational datasets are not fully public, limiting the granularity of statistical analysis, especially regarding demographic impacts and system error rates. Additionally, breach reporting in Pakistan remains inconsistent, which may understate the scale of data security incidents.

Future Research

Future studies should pursue longitudinal tracking of biometric misuse cases, drawing on court records, media reports, and civil society monitoring to evaluate systemic risks over time.

Moreover, comparative analysis with jurisdictions that have implemented robust biometric governance such as under the GDPR could provide actionable insights for policy design in Pakistan.

Conclusion

The aim of the study is to provide an understanding of the interplay between the use of biometric data, privacy rights, ethical factors, and legal provisions in Pakistan, taking into consideration both the empirical findings based on the usage pattern of biometrics in Pakistan by NADRA and the literature regarding data protection and its surveillance. It was found that biometric verification has had a steady and consistent upward trend since 2018 and is likely to continue moving upwards beyond 2024, along with an increase in complaints and data breaches. The operational and rights-related dangers associated with the increased use of biometric systems can be highlighted by the strong statistical correlation between biometric use and complaints ($r = 0.96$). The above results reinforce existing intellectual apprehensions that unless biometric technologies are anchored by strong protection mechanisms, they will stand to risk losing privacy, marginalization, and systemic compromises, despite their potential in preventing fraud and enhancing the efficiency of services delivered. The immutability of biometric identifiers exacerbates the impact of breaches and function creep resulting from the centralized NADRA infrastructure in Pakistan. Policy-wise, the findings suggest three areas of immediate concern: a statutory data protection act that takes into account the sensitivity of biometrics as data, an independent oversight system with accuracy and auditing mandates, and an easy-to-access redressal avenue that may include alternative authentication routes. This is needed to regain community confidence and to realign biometric government with constitutionally implied rights of dignity and privacy. The restrictions on data availability and inconsistencies in breach reporting presented in the study indicate the necessity of increased official transparency on the part of any institution. In future studies, longitudinal methods for monitoring instances of biometric misuse should be considered, collecting data on the efficiency of new legal means of protection. Finally, biometric growth presents both opportunities and challenges: it can lead to enhanced security and functional services; however, without full governance control, it can even backfire, enforcing bias that favors governments over human rights, often prioritizing surveillance and control. It involves creating a balance purposefully through legal reforms, technical precision, and a rights-based approach to technology adoption.

References

Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings*, *80*, 2642–2646.

Alyas, T., Almansour, B. Y., Tabassum, N., Almansour, A. Y., & Azhar, A. (2024). Enhancing Governance in Pakistan Through E-Government: The Role of Evidence-Based Monitoring Systems. *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, 1–10. https://ieeexplore.ieee.org/abstract/document/10836172/

Bennett, C. J. (2010). *The privacy advocates: Resisting the spread of surveillance*. Mit Press. https://books.google.com/books?hl=en&lr=&id=aKEPrhAtk7wC&oi=fnd&pg=PR7&dq=Bennett,+C.J.,+2018.+Privacy+Advocates:+Resisting+the+Spread+of+Surveillance.+MIT+Press.&ots=hiP2tWma6Z&sig=M-ARpXH1CDwdVMnJ1_mi9VemkRY

Bernal-Romero, J. C., Ramirez-Cortes, J. M., Rangel-Magdaleno, J. D. J., Gomez-Gil, P., Peregrina-Barreto, H., & Cruz-Vega, I. (2023). A review on protection and cancelable techniques in biometric systems. *Ieee Access*, *11*, 8531–8568.

Bhat, I. H. (2024). Legal Dimensions of Social Media Regulation in India: Challenges and Opportunities. *Journal of Society in Kashmir*, *14*(1), 102–120.

Bryman, A. (2016). *Social research methods*. Oxford university press. https://books.google.com/books?hl=en&lr=&id=N2zQCgAAQBAJ&oi=fnd&pg=PP1&dq=Bryman,+A.,+2016.+Social+Research+Methods.+5th+ed.+Oxford:+Oxford+University+Press.&ots=dqNvJRI6rg&sig=n1yvGvEw-SaxwGW6dV3F1K9X6zM

Bukhari, M., Sattar, S., Saleem, S., Khan, K. Z., & Khan, A. (2024). The Impact of Cybercrime Incidents and Artificial Intelligence adoption on Organizational Performance: A Mediation and moderation model. *Journal of Excellence in Social Sciences*, *3*(3), 191–210.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Conference on Fairness, Accountability and Transparency*, 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline&ref=akusion-ci-shi-dai-bizinesumedeia

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications.

Dove, E. S. (2018). The EU general data protection regulation: Implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics*, *46*(4), 1013–1030.

Field, A. (2024). *Discovering statistics using IBM SPSS statistics*. Sage publications limited. https://books.google.com/books?hl=en&lr=&id=83L2EAAAQBAJ&oi=fnd&pg=PT8&dq=Field,+A.,+2018.+Discovering+Statistics+Using+IBM+SPSS+Statistics.+5th+ed.+London:+SAGE.&ots=UbNUFlBJFJ&sig=CUO_hMikRcLdexhQxNwYUGHPA20

Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16). Springer Science & Business. https://books.google.com/books?hl=en&lr=&id=iqnBBAAAQBAJ&oi=fnd&pg=PA20&dq=Digital+Personal+Data+Protection+Act:&ots=2Yt61KPUL_&sig=y82mLdVH_FF5FRXTH0B_vVntHc0

Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Including Indonesia and Turkey (January 30, 2017)*, *145*, 10–13.

Haq, A. H. U. (2024). The right to privacy & personal data protection: An analysis of Pakistan's proposed personal data protection bill. *UCP Journal of Law & Legal Education*, *2*(2), 01–27.

Hashmi, Z. (2021). *Identifying Kin Biometric Belonging and Databased Governance in Colonial South Asia and Postcolonial Pakistan* [PhD Thesis]. https://deepblue.lib.umich.edu/handle/2027.42/171363

Hussain Danwar, S., Ahmed Mahar, J., & Kiran, A. (2022). A Framework for e-Voting System Based on Blockchain and Distributed Ledger Technologies. *Computers, Materials & Continua*, *72*(1). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15462218&AN=155538890&h=W%2BGKN8tyCapKJ7iIAItI88cdqGJoE0SYD1xK%2B0Bt64DjSonOQ5rC3JJ9gYV%2Fg5pXIK4U4tZ3C5RALGsg%2FlEiUg%3D%3D&crl=c

Jahangir, A. (2024). Governance Innovation in South Asia: The Pakistan Governance Journey. In *Mapping Governance Innovations* (pp. 147–166). Routledge India. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003506720-8/governance-innovation-south-asia-amir-jahangir

Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust, but verify. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(3), 303–323.

Manisha, & Kumar, N. (2020). Cancelable Biometrics: A comprehensive survey. *Artificial Intelligence Review*, *53*(5), 3403–3446. https://doi.org/10.1007/s10462-019-09767-8

Mukhija, K., & Jaiswal, S. (2023). Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR. *Jus Corpus LJ*, *4*, 638.

Nishat, S. (2022). *E-Government: Antecedents to Technology Adoption and Creating Public Value in Pakistan* [PhD Thesis, Victoria University]. https://vuir.vu.edu.au/44406/

Petrovic, M. (2024). Critical Review of the Personal Data Protection Act. *Pravni Horizonti*, *6*, 141.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Raizada, N., & Biswal, M. (2024). *Protecting Personal Health Information in Digital Age: Exploring Indian Legal Perspective*. https://www.irjms.com/wp-content/uploads/2024/07/Manuscript_IRJMS_0883_WS.pdf

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288–5303.

Salik, M. F., Mustafa, G., & Ali, A. (2025). Role of World Bank in Land Digitalization in Pakistan: An Analysis. *Journal of Politics and International Studies*, *11*(1), 65–86.

Tabachnick, B. G., & Fidell, L. S. (2007). *Experimental designs using ANOVA* (Vol. 724). Thomson/Brooks/Cole Belmont, CA. https://www.researchgate.net/profile/Barbara-Tabachnick/publication/259465542_Experimental_Designs_Using_ANOVA/links/5e6bb05f92851c6ba70085db/Experimental-Designs-Using-ANOVA.pdf

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal data protection law in digital banking governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1), 99–130.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203–213). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003320609-27/age-surveillance-capitalism-shoshana-zuboff