



Regulating Privacy Rights in the Global Data Governance: A Comparative Analysis of the Legal Framework of the United States and Pakistan

Ehsan Ul Haq

University Of Hertfordshire (UK), Master of Laws (LLM)

Email: ehsansaeed731@gmail.com

ABSTRACT

Modern technological advancement has substantially transformed the traditional understanding of privacy rights and created unprecedented legal challenges concerning the protection of personal information, digital communications, and informational autonomy. This study examines the legal protection of privacy rights in the digital era through a comparative analysis of the United States and Pakistan. It employs a qualitative and comparative legal research methodology and analyzes constitutional provisions, statutory frameworks, judicial decisions, international human rights instruments, and relevant scholarly literature governing digital privacy in both jurisdictions. It explores the philosophical foundations of privacy protection, regulation of personal data and surveillance, judicial approaches to digital privacy rights, and institutional enforcement mechanisms. The findings reveal that the United States possesses a relatively developed but fragmented privacy regime characterized by sector-specific legislation and extensive judicial interpretation, whereas Pakistan's legal framework remains underdeveloped and fragmented despite constitutional recognition of privacy under Article 14 of the Constitution. The comparative analysis further demonstrates significant differences in philosophical foundations, regulatory structures, judicial activism, and enforcement mechanisms. The study concludes by proposing legal and institutional reforms for strengthening digital privacy protection in Pakistan while identifying valuable lessons that both jurisdictions may derive from each other's legal experiences in addressing contemporary challenges of digital privacy and surveillance. Ultimately, the study makes a theoretical contribution to the development of effective global data governance frameworks.

Keywords: Digital Privacy Rights, Right to Privacy, Comparative Law, United States, Pakistan, Data Protection

Introduction

Background of the Study

The very notion of privacy rights has evolved significantly from its traditional understanding as protection against physical intrusion to a broader legal and human rights principle, which now also encompasses informational autonomy and digital self-determination. In the contemporary legal sense, the term privacy is commonly traced to the emergence of the notion of privacy as the “right to be let alone”. However, in this digital age, technological advancements such as artificial intelligence, social media platforms, cloud computing, and mass surveillance have fundamentally transformed the nature and scope of privacy concerns. This has made it inevitable that the legal systems must reconsider the traditional concepts of privacy protections (Diggelmann, 2014).



Vol. 4 No. 6 (Jun) (2026)

The abrupt increase in the collection, processing, and utilisation of personal data by state and private actors has made digital privacy one of the most significant legal and human rights challenges in the twenty-first century. However, endeavours to contain this challenge are also underway. Developed as well as developing jurisdictions are trying to adopt various approaches to protect digital privacy. Yet, there remain substantial differences among these regarding constitutional safeguards, statutory regulation, judicial interpretation, and enforcement mechanisms. In this regard, the United States has historically adopted a robust, sector-specific approach to privacy regulation, whereas developing countries such as Pakistan continue to develop comprehensive legal frameworks, with enormous digital challenges (Zang, 2024; Ul Haq, 2024).

Problem Statement

Despite legislative endeavours, the rapid expansion of digital technologies has outpaced the development of coherent legal frameworks governing privacy rights in many jurisdictions. In the United States, a robust constitutional tradition and numerous sector-specific statutes exist. However, there is an absence of a comprehensive federal data protection regime, which results in fragmented protections and regulatory inconsistencies. Similarly, questions regarding the adequacy of legal safeguards in protecting the privacy rights in this digital age are also fundamental, due to the growth of surveillance technologies, data analytics, and cross-border data transfers. (Serwin, 2009). In Pakistan, although Article 24 of the Constitution guarantees the dignity and privacy of individuals, the country's legal framework for digital privacy remains underdeveloped and fragmented. Existing legislation, including cybercrime and surveillance laws, lacks comprehensive data protection standards, effective oversight mechanisms, and adequate judicial remedies.

Although there exists enormous literature on the development of privacy rights in both the United States and Pakistan separately, there is a significant gap in comparative legal scholarship examining how Pakistan's evolving privacy framework compares with the more developed but fragmented legal regime of the United States. In particular, there is no research on the legal frameworks of the two jurisdictions for safeguarding privacy rights in this digital era, in the context of constitutional protections, statutory regulation, and judicial enforcement of digital privacy rights (Rana, 2025).

Research Questions

This study seeks to examine the legal protection of privacy rights in the digital age through a comparative analysis of the United States and Pakistan. It addresses the following research questions: (i) What are the constitutional, statutory, and judicial mechanisms governing digital privacy in the United States and Pakistan? (iii) What are the major similarities and differences between the privacy protection regimes of the two countries? (iv) How effective are their respective enforcement mechanisms and legal remedies? (v) What legal reforms can Pakistan and the US adopt to strengthen the protection of digital privacy rights, with respect to each other?

Research Objectives

Primarily, this study aims to conduct a comprehensive comparative legal analysis of digital privacy rights in the United States and Pakistan. Specifically, it aims at examining the conceptual and legal foundations of digital privacy rights in the two jurisdictions, in the context of the constitutional, statutory, and judicial frameworks. Furthermore, it identifies similarities, differences, strengths, and weaknesses within their respective legal



Vol. 4 No. 6 (Jun) (2026)

systems and evaluates the effectiveness of enforcement mechanisms and remedies. Ultimately, it proposes practical and context-specific legal recommendations for strengthening Pakistan's digital privacy framework, in light of the advanced US legal framework.

Conceptual Framework of Digital Privacy Rights

The Evolution of Privacy as a Human Right

The evolution of the concept of privacy has experienced a journey from a narrow protection against physical intrusion to a comprehensive human right encompassing personal autonomy, dignity, and informational self-determination. In previous eras of human history, privacy protections existed primarily in domestic constitutional systems, which used to focus on the inviolability of the home and correspondence. However, after the Second World War, privacy emerged as an internationally recognized human right through the development of global human rights instruments. Therefore, Diggelmann and Cleis (2014) argue that the recognition of privacy as a universal human right represented a significant shift from traditional legal protections to a broader conception of individual liberty and human dignity.

This evolution of privacy has been further accelerated by the technological advancement and digitalization of human society. Current legal debates explicitly recognize privacy not merely as a negative right against state interference but also as a positive right essential for personal identity, autonomy, and democratic participation. Such a legal understanding of privacy has become increasingly dynamic and contextual, adapting to the changing social and technological realities of modern societies, particularly in the context of digital communication and information processing (Baghai, 2012).

Privacy Rights under International Human Rights Law

Under international human rights law, the notion of Privacy rights enjoys an explicit and extensive recognition. The Universal Declaration of Human Rights (UDHR) provides that no person shall be subjected to arbitrary interference with their privacy, family, home, or correspondence (UDHR, Article 12). Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) establishes the right to protection against arbitrary or unlawful interference with privacy and obligates states to provide legal protection against such interference. These provisions have transformed privacy from a domestic constitutional principle into a universally recognized human right with international legal significance.

In the context of technological developments and digital surveillance practices, the interpretation of privacy rights under international law has evolved considerably. For instance, the United Nations Human Rights Committee has interpreted Article 17 of the ICCPR to encompass the protection of personal data, electronic communications, and digital information processing. International human rights law now recognizes that the collection, storage, and use of personal information by both public and private actors must be subject to legality, necessity, proportionality, and effective safeguards to prevent arbitrary interference with individual privacy rights (Taylor, 2020).

The Concept of Digital Privacy in the Information Age

In the virtual environment of the contemporary technological era, the idea of privacy has been transformed from just a mere physical concept into a multidimensional digital right involving the collection, processing, storage, and dissemination of personal information. Comprehensively, digital privacy encompasses the protection of personal data, online



Vol. 4 No. 6 (Jun) (2026)

communications, internet activities, biometric information, and algorithmic profiling. The emergence of digital platforms, artificial intelligence, and big data computing has created unprecedented opportunities for surveillance and data exploitation. This scenario inevitably necessitates stronger legal protections for individual privacy rights (Yeung, 2018).

Now, various legal jurisdictions view the protection of digital privacy as a fundamental prerequisite for preserving personal autonomy, democratic participation, and human dignity. With the increase in surveillance capitalism, concerns regarding the adequacy of existing legal frameworks have intensified. Digital surveillance by both governmental and private entities presents significant challenges to traditional privacy doctrines and requires comprehensive regulatory responses capable of addressing emerging technological risks (Solove, 2025; Mallard, 2022).

Research Methodology

This study adopts a qualitative doctrinal and comparative legal research methodology to examine the protection of privacy rights in the digital age within the legal frameworks of the United States and Pakistan. It resorts to both primary and secondary data. Primary legal sources, including constitutional provisions, statutes, judicial decisions, international human rights instruments, and relevant regulatory frameworks governing digital privacy rights in both jurisdictions has been analyzed. In particular, the study examines the Fourth Amendment to the Constitution of the United States, federal and state privacy legislation, Article 14 of the Constitution of Pakistan, the Prevention of Electronic Crimes Act, 2016, and relevant judicial pronouncements concerning privacy and surveillance. The research also relies upon secondary sources, which mainly include peer-reviewed journal articles, legal commentaries, and academic literature. The doctrinal method remains one of the most appropriate methodologies for analysing legal principles, judicial interpretation, and statutory frameworks within comparative legal scholarship.

Furthermore, via comparative legal method, it compares how the United States and Pakistan address similar legal problems relating to digital privacy, including governmental surveillance, personal data protection, digital communications, and enforcement mechanisms. It identifies the similarities, differences, strengths, and weaknesses of the two legal systems by focusing on how each jurisdiction responds to comparable social and legal challenges rather than merely comparing legal texts. The comparative analysis is conducted at constitutional, statutory, judicial, and institutional levels to evaluate the effectiveness of existing legal frameworks and identify potential reforms for strengthening privacy protection in Pakistan. This methodological approach enables a contextual and critical examination of digital privacy rights and provides a sound basis for proposing practical legal reforms informed by comparative experience

The Legal Framework for Privacy in the United States

The constitutional guarantee

In the United States legal framework, the primary foundation of privacy protection is derived from the Fourth Amendment to the U.S. Constitution. This amendment guaranteed the right of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Although it does not expressly mention the very term privacy, the U.S. Supreme Court has interpreted the Fourth Amendment as providing significant protection against governmental intrusion. In *Katz v. United States* (1967), the Court established the "reasonable expectation of privacy"



Vol. 4 No. 6 (Jun) (2026)

test, fundamentally transforming constitutional privacy jurisprudence. Scholars have argued that *Katz* shifted Fourth Amendment protection from property-based concepts to a broader understanding of personal privacy rights (Kahn-Fogel, 2020).

In fact, the advances of digital technologies forced courts to reinterpret Fourth Amendment protections in light of modern surveillance practices. In *Carpenter v. United States*, 585 U.S. 296 (2018), the Supreme Court held that law enforcement generally requires a warrant to access historical cell-site location information, thereby limiting the traditional third-party doctrine. This decision demonstrates a significant development in constitutional privacy law by recognizing that individuals retain privacy interests in certain forms of digital data shared with third parties. This decision has substantially reshaped Fourth Amendment jurisprudence in the digital era and expanded constitutional safeguards for electronic information (Tokson, 2022).

Sectoral approach of the federal statutory framework

Many jurisdictions have adopted comprehensive privacy-related legislation. However, the United States has developed a sector-specific regulatory framework for privacy protection. Federal privacy regulation consists of multiple statutes governing particular industries and categories of information, including the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm-Leach-Bliley Act (GLBA) of 1999, the Children's Online Privacy Protection Act (COPPA) of 1998, and the Electronic Communications Privacy Act (ECPA) of 1986. This sectoral approach reflects the American preference for sector-specific regulation rather than comprehensive data protection legislation (Solove, 2022).

However, such a sector-specific model may create inconsistencies, regulatory gaps, and uneven levels of protection across different categories of personal data. Financial institutions, healthcare providers, educational institutions, and internet service providers remain subject to different legal obligations and enforcement mechanisms. Such overlapping federal and state privacy requirements have created significant compliance challenges and consumer confusion. This fragmented structure of privacy law may undermine transparency and complicate effective privacy protection in the digital economy (Xian, 2025).

State-level legislation

As the US has a sector-specific framework for privacy rights, and there is no comprehensive federal privacy legislation, several states have enacted their own privacy laws, with California emerging as the leading jurisdiction in this area. The California Consumer Privacy Act (CCPA) of 2018, subsequently amended by the California Privacy Rights Act (CPRA) of 2020, provided extensive rights relating to personal information, including the rights to access, delete, correct, and opt out of the sale of personal data. It demonstrates one of the most comprehensive state-level privacy regimes in the United States and has significantly influenced legislative developments in other states (Nguyen, 2022). California Privacy Rights Act (CPRA) shows a shift toward recognizing privacy as a fundamental consumer and civil right rather than merely a commercial concern. The establishment of the California Privacy Protection Agency (CPPA) has further strengthened enforcement and regulatory oversight mechanisms. However, substantial gaps exist in organizational compliance, and stronger enforcement mechanisms remain necessary to ensure the effectiveness of state privacy legislation (Gueorguieva et al., 2026).



Vol. 4 No. 6 (Jun) (2026)

Enforcement and Remedies

In terms of the enforcement of privacy rights regulations in the US, it involves a complex combination of federal agencies, state regulators, and judicial remedies. At the federal level, the Federal Trade Commission (FTC) exercises broad authority under Section 5 of the Federal Trade Commission Act of 1914 to prohibit unfair or deceptive practices relating to consumer privacy and data security. Additionally, sector-specific agencies such as the Department of Health and Human Services enforce statutes such as HIPAA. The decentralized nature of privacy enforcement has contributed to regulatory fragmentation and varying levels of protection across sectors (Solove, 2022).

Judicial remedies for privacy violations in the United States include constitutional claims, statutory damages, injunctions, administrative penalties, and private causes of action, which were authorized by legislation. Constitutional remedies under the Fourth Amendment typically require exclusion of unlawfully obtained evidence through the exclusionary rule. However, existing enforcement mechanisms often face challenges in providing effective remedies for large-scale digital privacy violations. Knox (2020) argues that modern digital surveillance practices have exposed significant limitations in traditional constitutional remedies and underscore the need for more comprehensive enforcement frameworks.

The Legal Framework for Privacy in Pakistan

The Constitutional Foundation

In Pakistan, the basic source of the right to privacy is Article 14(1) of the Constitution of the Islamic Republic of Pakistan 1973. It ensures that "the dignity of man and, subject to law, the privacy of home, shall be inviolable". Nevertheless, the Constitution does not expressly recognize a general right to informational privacy. However, superior courts have often interpreted the guarantee of dignity and privacy broadly to encompass protection against arbitrary state intrusion. This article has evolved from a traditional protection of physical spaces into a constitutional safeguard capable of addressing emerging digital privacy concerns and informational autonomy in the age of surveillance technologies (Ul Haq, 2024). International human rights norms have also influenced the constitutional understanding of privacy in the country. For instance, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) is substantial in this regard, to which Pakistan is a state party. Legal literature in Pakistan has always stressed that Article 14 should be interpreted dynamically to include personal data protection, electronic communications, and protection against disproportionate digital surveillance (Jamil et al., 2025).

The Statutory Framework

In a broad sense, Pakistan's statutory framework for governing digital privacy is not comprehensive. Rather, it remains fragmented and primarily consists of the Prevention of Electronic Crimes Act (PECA), 2016, the Investigation for Fair Trial Act, 2013, and sector-specific regulations. PECA, 2016, is the principal legislative instrument which regulates cybercrime, unauthorized access to information systems, identity theft, cyberstalking, and electronic surveillance. Although, PECA contains certain privacy-related protections, it primarily adopts a security-oriented approach rather than establishing a comprehensive framework for personal data protection and informational privacy (Haider et al., 2023).

The absence of comprehensive data protection legislation is generally considered one of the most significant gaps in Pakistan's digital framework. Although the Personal Data



Vol. 4 No. 6 (Jun) (2026)

Protection Bill has undergone several revisions, it has yet to be enacted into law. Existing legal mechanisms provide limited protection regarding consent, data processing, cross-border data transfers, and the rights of data subjects. As a result, the current statutory framework lacks international data protection standards and remains inadequate to address contemporary challenges posed by digital technologies, artificial intelligence, and surveillance capitalism (Ul Haq, 2024; Rana & Iqbal, 2025).

The Role of the Judiciary

The Superior judiciary of Pakistan has played a significant role in interpreting and expanding the constitutional dimensions of privacy rights. The courts have consistently recognized that the constitutional guarantee of human dignity under Article 14 extends beyond physical privacy and encompasses broader personal liberties. Judicial interpretation has increasingly acknowledged the necessity of balancing state interests in security and law enforcement with individual rights to privacy, due process, and informational autonomy (Qasim et al., 2026).

This crucial role of the judiciary is evident from its past decisions. For instance, in *Mohtarma Benazir Bhutto v. President of Pakistan*, the Supreme Court held that the right to life must be considered as a sacred right "which cannot be violated, discriminated against, or abused by any authority. It recognized that unauthorized telephone tapping and electronic surveillance constitute violations of the constitutional guarantees of dignity and privacy under Article 14 of the Constitution. This landmark judgment established an important constitutional foundation for privacy jurisprudence in Pakistan and continues to influence judicial approaches to digital surveillance and informational privacy. Similarly, in *Sh. Liaquat Hussain and others v. Federation of Pakistan*, it was declared that this right must not be denied even to the terrorists (Jabeen, 2021).

In the context of digital privacy, courts have been required to address challenges arising from electronic surveillance, cybercrime investigations, and state regulatory powers under PECA, 2016. Judicial decisions have demonstrated a cautious approach toward balancing technological regulation with constitutional guarantees. However, Pakistan has yet to develop a coherent and comprehensive doctrine of digital privacy comparable to advanced constitutional jurisdictions. The absence of consistent judicial standards has consequently limited the development of robust privacy jurisprudence in the digital sphere (Rana & Iqbal, 2025; Qasim et al., 2026).

Enforcement and Challenges

The enforcement of privacy rights in Pakistan is primarily carried out through various institutions. These institutions mainly include the Federal Investigation Agency (FIA), the Pakistan Telecommunication Authority (PTA), and the ordinary courts. Under PECA, 2016, the FIA's National Response Centre for Cyber Crime (NR3C) serves as the principal investigative body responsible for cybercrime and privacy-related offenses. Nevertheless, scholars have identified significant institutional weaknesses, including inadequate technical expertise, procedural inefficiencies, and insufficient oversight mechanisms, which undermine the effective enforcement of privacy protections (Shah, 2024).

Pakistan's digital privacy regime also faces broader structural challenges arising from expanding state surveillance powers, technological developments, and the absence of comprehensive personal data protection legislation. Such excessive reliance on security-oriented legislation, coupled with inadequate safeguards against arbitrary surveillance and limited judicial remedies, has created substantial concerns regarding the protection



Vol. 4 No. 6 (Jun) (2026)

of fundamental privacy rights. Therefore, Pakistan requires a comprehensive, rights-based data protection framework supported by independent regulatory oversight and stronger constitutional safeguards (Ul Haq, 2024).

Comparative Analysis

Philosophical and Constitutional Foundations

The foremost aspect in which the United States' and Pakistan's jurisdictions differ is the philosophical foundations of privacy protection, including their constitutional origins and legal evolution. In the United States, privacy has developed primarily through a liberal tradition emphasizing individual autonomy and protection against state intrusion. In a broader sense, the judicial interpretation of constitutional provisions, particularly the Fourth Amendment, took place under this umbrella. Landmark decisions like *Katz v. United States* and extending to *Carpenter v. United States*, reflect an understanding of privacy as a constitutional liberty interest grounded in personal autonomy and freedom from unreasonable governmental surveillance. American privacy law remains deeply rooted in constitutional liberalism and the protection of individual liberty rather than in comprehensive data protection principles (Richards, 2020; Boyne, 2018).

In contrast, Pakistan derives its privacy principle from the concepts of human dignity and the inviolability of private life, as embodied in Article 14 of the Constitution of Pakistan, 1973. Unlike the United States, where privacy evolved through liberal tradition, Pakistan's principle of privacy has developed within the broader framework of constitutional guarantees of dignity, personal liberty, and international human rights obligations. Pakistan's emerging digital privacy framework increasingly incorporates human rights-based approaches to informational privacy while simultaneously balancing concerns of national security and public order (Rana & Iqbal, 2025).

Differences in regulatory frameworks

There exists a substantial difference in regulatory frameworks governing digital privacy in the United States and Pakistan. The United States' framework is a sector-specific approach consisting of federal statutes such as HIPAA, COPPA, GLBA, and ECPA, supplemented by state legislation such as the California Consumer Privacy Act (CCPA). This decentralized model shows the American preference for sectoral regulation and market-oriented governance rather than comprehensive national legislation. Although this approach allows regulatory flexibility, it simultaneously creates inconsistencies, regulatory gaps, and uneven protections across different sectors and categories of personal information (Solove, 2006).

Unlike this sector-specific approach, Pakistan lacks a comprehensive data protection regime and instead relies upon a combination of constitutional guarantees and national laws like the Prevention of Electronic Crimes Act, 2016. Despite ongoing efforts to enact comprehensive personal data protection legislation, Pakistan's existing framework remains fragmented and heavily focused on cybersecurity and surveillance concerns. The absence of an independent data protection authority and comprehensive statutory protections significantly weakens Pakistan's ability to safeguard digital privacy rights effectively (Ul Haq, 2024).

Comparing Key Legal Principles

Regarding the substantive legal principles governing privacy rights, there exist both convergent and divergent aspects between the two. The United States deals with privacy protection primarily through doctrines such as reasonable expectation of privacy,



Vol. 4 No. 6 (Jun) (2026)

consent, procedural due process, and restrictions on unreasonable searches and seizures. The Judiciary has also interpreted it in the same direction by defining the scope of these principles, particularly in relation to emerging technologies and digital surveillance practices. The American legal system continues to prioritize individual liberty and constitutional procedural protections over comprehensive informational self-determination (Rehm, 2001).

On the other hand, Pakistan's legal framework recognizes principles such as legality, necessity, proportionality, and judicial oversight, primarily through constitutional interpretation and international human rights obligations. However, these principles remain inconsistently applied due to legislative gaps and limited judicial development of digital privacy doctrines. While Pakistan has formally adopted several international privacy principles, their practical implementation and enforcement remain substantially weaker than those found in developed jurisdictions (Jamil & Thakur, 2026).

Divergences in enforcement and remedies

The two jurisdictions also reflect differences in the institutional and procedural enforcement mechanisms. The United States primarily conducts privacy enforcement through multiple federal agencies, including the Federal Trade Commission (FTC), state regulatory authorities, private litigation, and constitutional remedies available through judicial review. The FTC has emerged as one of the most influential institutions regulating digital privacy through its authority to prohibit unfair and deceptive business practices. Nevertheless, despite the fragmented regulatory structure, the availability of multiple enforcement mechanisms provides relatively robust remedial protections for privacy violations (Solove 2014).

In contrast, Pakistan's enforcement framework remains institutionally fragmented and comparatively weak. Enforcement responsibilities are primarily vested in the Federal Investigation Agency, the Pakistan Telecommunication Authority, and ordinary courts. However, institutional deficiencies, including limited technical expertise, inadequate regulatory oversight, insufficient judicial remedies, and broad executive discretion in surveillance matters. As a result, the absence of an independent supervisory authority and comprehensive data protection legislation continues to undermine effective enforcement of digital privacy rights in Pakistan.

Judicial Activism vs. Judicial Restraint

The role of the judiciary in developing privacy rights demonstrates a fundamental contrast between the United States and Pakistan. Historically, the United States Supreme Court has played an active role in developing constitutional privacy doctrines through landmark decisions such as *Katz v. United States* and *Carpenter v. United States*. Through judicial interpretation, American courts have continuously adapted constitutional protections to address technological developments and evolving societal expectations of privacy. Comparative constitutional scholars argue that judicial activism has been essential to the development of American privacy jurisprudence, particularly in the absence of comprehensive federal privacy legislation (Rehm, 2001).

In Pakistan, although the judiciary has played an important role in protecting constitutional rights through judicial review and suo motu jurisdiction, courts have generally adopted a more cautious approach toward developing comprehensive digital privacy jurisprudence. Decisions such as *Mohtarma Benazir Bhutto v. President of Pakistan* established important constitutional principles concerning privacy and surveillance; however, judicial intervention in digital privacy matters remains



Vol. 4 No. 6 (Jun) (2026)

comparatively limited. Legal scholars argue that while judicial activism has expanded constitutional rights in several domains, Pakistan's courts have yet to establish a coherent and systematic body of digital privacy jurisprudence comparable to that of the United States (Cheema, 2016; Idrees et al., 2026).

Reciprocal Recommendations

This comparative analysis reveals that although the United States and Pakistan have adopted significantly different approaches to digital privacy protection, both jurisdictions face important legal and institutional challenges. The United States possesses a relatively developed but fragmented privacy regime characterized by constitutional safeguards, sector-specific legislation, and extensive judicial interpretation. Pakistan, on the other hand, recognizes privacy as a constitutional right but lacks a comprehensive statutory and institutional framework capable of effectively addressing the challenges posed by digital technologies. Therefore, both jurisdictions can benefit from each other's experiences and adopt corresponding legal reforms to strengthen the protection of digital privacy rights.

Recommendations for Pakistan from the United States Experience

Pakistan can draw several important lessons from the legal and institutional development of privacy rights in the United States. First, Pakistan should enact a sector-specific personal data protection law that clearly defines the rights and obligations of data subjects, public authorities, and private entities. The United States' extensive regulatory framework demonstrates the importance of establishing detailed legal protections for various forms of personal information.

Second, Pakistan should establish an independent and autonomous data protection authority with adequate regulatory and enforcement powers. The comparative experience of the United States demonstrates the significance of specialized institutions such as the Federal Trade Commission in enforcing privacy protections and regulating digital markets. Pakistan should similarly create a specialized supervisory body responsible for monitoring compliance, investigating violations, issuing regulations, and imposing administrative sanctions.

Third, Pakistan's judiciary should adopt a more dynamic and progressive approach toward constitutional interpretation of privacy rights. The judicial development of privacy doctrines in the United States, particularly through landmark decisions concerning electronic surveillance and digital information, demonstrates the important role courts can play in protecting privacy rights in rapidly changing technological environments.

Furthermore, Pakistan should strengthen institutional oversight of surveillance practices and establish effective judicial remedies for privacy violations. Surveillance activities should be subjected to independent authorization, proportionality requirements, and judicial review. Enhanced public awareness campaigns, digital literacy programs, and institutional capacity building should also be introduced to strengthen the practical protection of digital privacy rights.

Recommendations for the United States from Pakistan's Experience

Although the United States possesses a more advanced legal framework for digital privacy protection, certain features of Pakistan's constitutional approach provide valuable lessons for the American legal system. First, the United States may consider recognizing privacy more explicitly as a fundamental constitutional and human rights value rather than relying primarily upon fragmented statutory protections. Pakistan's constitutional



Vol. 4 No. 6 (Jun) (2026)

emphasis on human dignity provides a broader normative foundation for privacy protection, which may offer valuable guidance for future constitutional and legislative reforms in the United States.

Similarly, the United States may benefit from strengthening federal oversight and creating a specialized national data protection authority with comprehensive regulatory authority. Existing enforcement mechanisms remain dispersed among multiple federal and state agencies, resulting in overlapping jurisdictions and inconsistent enforcement practices. A centralized supervisory institution could improve regulatory coherence, enhance enforcement efficiency, and provide stronger protection against emerging technological threats.

In sum, both jurisdictions should recognize that digital privacy protection requires a balanced approach that safeguards individual autonomy, human dignity, technological innovation, and national security interests. Continued comparative legal engagement and mutual learning between developed and developing legal systems remain essential for addressing the increasingly complex challenges of privacy protection in the digital age.

Conclusion

In conclusion, digital advancements have substantially transformed the traditional understanding of privacy rights and have created unprecedented challenges for legal systems across the world. Systematic comparison of the constitutional, statutory, judicial, and institutional frameworks governing digital privacy rights in the United States and Pakistan reveals that although the United States possesses a relatively mature and sophisticated privacy framework, its regulatory structure remains fragmented and inconsistent. Conversely, Pakistan recognizes privacy as a fundamental constitutional right through Article 14 of its Constitution but continues to face significant challenges arising from legislative gaps, institutional weaknesses, limited judicial development, and inadequate enforcement mechanisms.

Therefore, neither jurisdiction offers a perfect model for digital privacy protection. Nevertheless, each provides valuable lessons for the other. While Pakistan can benefit from the institutional development, judicial innovation, and enforcement mechanisms of the United States, the American legal system may also draw important insights from Pakistan's constitutional emphasis on human dignity and fundamental rights. In short, effective protection of privacy rights in the digital age requires comprehensive legislation, independent oversight institutions, robust judicial protection, effective remedies, and a continued commitment to balancing technological innovation with the preservation of human dignity, personal autonomy, and democratic values.

References

- Baghai, K. (2012). Privacy as a human right: A sociological theory. *Sociology*, 46(5), 951-965. <https://doi.org/10.1177/0038038512450804>
- Boyne, S. M. (2018). Data protection in the United States. *The American Journal of Comparative Law*, 66(Suppl. 1), 299-343.
- Carpenter v. United States*, 585 U.S. 296 (2018)
- Constitution of the Islamic Republic of Pakistan*, 1973, art. 14(1) (Pak.).
- Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a human right. *Human Rights Law Review*, 14(3), 441-458. <https://doi.org/10.1093/hrlr/ngu014>
- Gueorguieva, A.-M., King, J., Panidapu, A., & Ho, D. E. (2026). *Privacy without remedy: An assessment of data broker compliance with California privacy law*.
- Haider, W., Ali, A., & Zubair, M. (2023). *Prevention of Electronic Crime Act, 2016: An*



Vol. 4 No. 6 (Jun) (2026)

- analysis of the act's effectiveness in controlling misuse of social media in Pakistan.* Journal of Educational Research and Social Sciences Review, 3(2).
- Jamil, M. S., Dayal, A. A., Bilal, H., & Qaiser, M. N. (2025). *Privacy of home to privacy-by-design: Article 14 of the Pakistani Constitution in the age of AI surveillance.* International Research Journal of Arts, Humanities and Social Sciences.
- Jamil, M. S., & Thakur, S. A. (2026). Privacy jurisprudence in Pakistan: Doctrinal IRAC analysis of Article 14 and PECA. Pakistan Journal of Social Science Review, 5(2), 449-469.
- Kahn-Fogel, N. A. (2020). *Katz, Carpenter, and classical conservatism.* Cornell Journal of Law and Public Policy, 29(1), 55-98.
- Katz v. United States, 389 U.S. 347 (1967).
- Knox, R. (2020). Fourth Amendment protections of health information after *Carpenter v. United States*: The devil's in the database. *American Journal of Law & Medicine*, 45(4), 427-455. <https://doi.org/10.1177/0098858819892744>
- Mallard, G. (2022). Critical theory in the age of surveillance capitalism: How to regulate the production and use of personal information in the digital age. *Law & Social Inquiry*, 47(1), 339-345.
- Mohtarma Benazir Bhutto and another v. President of Pakistan and others PLD 1998 SC 388
- Nguyen, T. (2022). *An empirical evaluation of the implementation of the California Consumer Privacy Act (CCPA).*
- Qasim, R., Hussain, N., & Jameel, M. S. (2026). *Judicial interpretation and case laws on right to privacy and the Prevention of Electronic Crimes in Pakistan.* Journal for Current Sign, 3(2), 1074–1082.
- Rana, A., & Iqbal, A. (2025). Privacy and surveillance: Legal and technical perspectives. *UCP Journal of Law & Legal Education*, 3(2). <https://doi.org/10.24312/ucp-jlle.03.02.552>
- Rehm, G. M. (2000). Just judicial activism? privacy and informational self-determination in us and german constitutional law. *Privacy and Informational Self-Determination in US And German Constitutional Law (January 23, 2000).*
- Richards, Neil M., and Woodrow Hartzog. "Privacy's Constitutional Moment and the Limits of Data Protection." *Boston College Law Review* 61.5 (2020): 1687.
- Serwin, A. B. (2009). Privacy 3.0: The principle of proportionality. *Michigan Journal of Law Reform*, 42(4), 869–955.
- Shah, S. K. A. (2024). *A critical analysis of efficacy of the Prevention of Electronic Crimes Act, 2016: Irritants and remedies.* Journal of Pakistan Administration, 45(2), 66–91.
- Sh. Liaquat Hussain and others v. Federation of Pakistan through Ministry of Law, Justice and Parliamentary Affairs, Islamabad and others PLD 1999 SC 504.
- Solove, D. J. (2025). Privacy in authoritarian times: Surveillance capitalism and government surveillance. *Boston College Law Review*, 66(1), 1-38.
- Solove, D. J. (2006). A model regime of privacy protection.
- Solove, D. J., & Hartzog, W. (2022). The FTC and the new common law of privacy. *Columbia Law Review*, 122(3), 583-676.
- Taylor, P. M. (2020). Article 17: Privacy, home, correspondence; honour and reputation. In *A commentary on the International Covenant on Civil and Political Rights* (pp. 458-498). Cambridge University Press. <https://doi.org/10.1017/9781108689458.020>



Vol. 4 No. 6 (Jun) (2026)

- Tokson, M. (2022). The aftermath of *Carpenter*: An empirical study of Fourth Amendment law, 2018-2021. *Harvard Law Review*, 135(7), 1790-1853.
- United Nations. (1948). *Universal Declaration of Human Rights*. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
- United Nations. (1966). International Covenant on Civil and Political Rights. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Ul Haq, A. H. (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). <https://doi.org/10.24312/ucp-jlle.02.02.122>
- Xian, L., Tran, V., Lee, L., Kumar, M., Zhang, Y., & Schaub, F. (2025). Layered, overlapping, and inconsistent: A large-scale analysis of the multiple privacy policies and controls of U.S. banks. *Proceedings on Privacy Enhancing Technologies*.
- Yeung, K. (2018). Five fears about mass predictive personalization in an age of surveillance capitalism. *International Data Privacy Law*, 8(3), 258-269. <https://doi.org/10.1093/idpl/ipy020>
- Zang, D. (2024). The Privacy Act of 1974: The American Bill of Rights on data and its unfinished business. *University of Pittsburgh Law Review*, 85(2). <https://doi.org/10.5195/lawreview.2024.1051>