# Pakistan's Digital Privacy : The End of Self-Regulation

**Barrister Zafar Iqbal Kalanauri**
Advocate Supreme Court of Pakistan[i]

## Abstract

Today, "data protection" and "digital privacy" are often used interchangeably. With advancing technology and tech companies increasingly intruding on individual privacy, the demand for strong data protection measures and comprehensive frameworks is on the rise. Developing nations like Pakistan, lacking a legal framework to regulate data-hoarding corporations, are particularly vulnerable. This article examines Pakistan's constitutional stance on privacy and related laws, evaluates the country's current data protection framework, and reviews recent regulatory efforts such as the drafting of the Personal Data Protection Bill 2021. Additionally, it compares Pakistan's approach to data protection with established laws like the EU's General Data Protection Regulation (GDPR) and the US's California Consumer Privacy Act (CCPA), to suggest steps that align with Pakistan's unique regulatory needs and consumer expectations.

## Introduction

In today's world, privacy is indispensable. While developed nations face challenges in understanding and enforcing privacy rights, countries like Pakistan confront heightened risks due to inadequate protections for their citizens. Though the underlying concerns about digital privacy are universal, the protective measures differ significantly, making the discussion around Pakistan's stance essential.

Pakistan's Constitution safeguards citizens' rights to privacy and dignity. Article 14 of the Constitution of the Islamic Republic of Pakistan (1973) states, "the dignity of man and, subject to law, the privacy of home, shall be inviolable."[1] This right is not absolute, however, and its interpretation in digital contexts poses new questions about state and private intrusions into individual privacy. Understanding these limits within the physical realm is crucial to extending them into the digital sphere.

## Key Judicial Rulings on Privacy Rights

Pakistan's courts have explored the right to privacy and its limitations in several significant cases, primarily in relation to state intervention. These rulings establish principles that can guide digital privacy protections.

## The "Privacy of Home" Paradox

[1] The Constitution of Pakistan 1973, Article 14.

The landmark case of *Mohtarma Benazir Bhutto v. President of Pakistan*[2] examined privacy within state surveillance, specifically phone call interception among public officials. Here, the Court broadened the definition of "home" to protect an individual's privacy beyond literal home spaces, drawing from the US Supreme Court's *Katz v. United States* ruling[3]. Justice Saleem Akhtar emphasized that privacy extends beyond the home, warning that a violation of personal privacy also impedes freedom of speech, closely tying privacy to expression in the digital context. The Court's decision integrated multiple constitutional rights with Article 14, underscoring privacy's significance within fundamental rights. This case set an important precedent that was referenced in subsequent rulings, including *Kh. Ahmad Tariq Raheem v. Federation of Pakistan*.[4]
In the *Mohtarma Benazir Bhutto* case, the Court deemed surveillance unconstitutional and contrary to Islamic teachings as outlined in Surah Al-Hujurat. Article 227 of the Constitution mandates that all laws align with Islamic principles, reinforcing that privacy violations breach not only constitutional but also religious principles, thus making any future encroachment unconstitutional under Article 227.

> The dignity of man and privacy of the home is inviolable, it does not mean that except in home, his privacy is vulnerable and can be interfered or violated.[5]

**Privacy as "Subject to Law"**

Despite these rulings, Article 14 qualifies privacy as "subject to law," signaling that privacy is not an absolute right. The degree of restriction needs careful examination, especially when applied to state and private actions.

In *Riaz v. Station House Officer*[6], a raid based on a warrant issued under the Code of Criminal Procedure (CrPC) was deemed unconstitutional as it was granted without sufficient consideration, violating the home's privacy. This decision, upheld in numerous cases, showed that even when prosecuting Hadd crimes like Zina, privacy remains a protected constitutional right. The *Zeeshan Ahmed v. The State*[7] and *Nadeem v. The State* cases further underscored this by invoking Islamic teachings that advocate respect for individual privacy, prioritizing it even in the face of serious allegations.

The Court held a raid conducted without a warrant to be unconstitutional and illegal. Furthermore, the Court cited two verses of the Holy Qur'an to highlight the importance of the right to privacy in Islam. Similarly, in *Nadeem v. The State,* Justice Khurshid Anwar Bhinder stressed the significance of the right to privacy by invoking Islamic teachings and principles. Justice Bhinder quoted the following Hadith in the Judgment:

---

[2] PLD 1998 Supreme Court 388.
[3] 389 U.S. 347.

[4] Ibid [29].
[4] 389 U.S. 347.
[5] Mohtarma Benazir Bhutto (n 2) [29].
[6] PLD 1998 Lah 35.

[7] 2007 YLR 1269.

> Holy Prophet (peace be upon him) had said that if you go to somebody's house knock the door once and if there is no reply knock it again and if there is no reply knock it for the third time and if still there is no reply, then do not try to enter the house and go back.[8]

Justice Qazi Faez Isa expanded on these principles, arguing that privacy extends beyond the home to public spaces, with individuals entitled to a reasonable expectation of privacy in all settings. This nuanced interpretation supports the need for strong privacy protections against intrusions by both the state and large private tech companies.[9]

**Why Regulate Big Data and Big Tech?**

For a long time, large tech companies collected massive amounts of data without state oversight, until both users and regulators recognized the risks involved. This section examines the harms associated with big data and big tech, arguing why regulation is essential as self-regulation falls short.

Shoshana Zuboff theorizes that tech corporations initially maintained a balanced relationship with users, where both learned from each other in a feedback loop. However, with the rise of targeted advertising, these companies evolved into entities driven by power and profit. Rather than storing user data randomly, companies began profiling users by associating data with individual identities and manipulating it in various ways, creating a significant power imbalance. A striking example is Target Corporation's ability to predict a customer's pregnancy based solely on purchasing pattern-such as scent-free lotions and supplements-demonstrating the disturbing predictive capabilities of corporations. This case heightened awareness about the sheer volume and nature of data collected, processed, and stored, often with users' consent. Understanding this interplay of consent, information, and power imbalance is crucial in today's digital age.

**Information Asymmetry and the Issue of Consent**

Information asymmetry occurs when one party in a transaction holds significantly more relevant knowledge than the other. In the case of big tech, this asymmetry is particularly evident in the "notice-and-choice" model used for obtaining user consent. Under this model, platforms present users with terms of service outlining data collection and usage, which users must accept to use the service. The approach aims to promote autonomy and choice by enabling individuals to consent freely to data practices. In

---

[8] 2009 PCrLJ 744, [7].

[9] *Chamber of Commerce and Industry Quetta Balochistan through Deputy Secretary v. Director General Quetta Development Authority* PLD 2012 Bal 31, [9].

theory, notice-and-choice embodies the concept of privacy and assumes that individual decisions will create a balance between privacy and the benefits of data use.

However, this approach presumes that users fully understand the terms provided by platforms, which is often not the case. The notices are typically complex, lengthy, and filled with legal jargon. As a result, most users, even those with higher education, tend to skim or entirely skip the terms, thus agreeing to conditions they may not fully understand. In a survey conducted for this paper, over 200 respondents, many of whom had completed at least a bachelor's degree, indicated that they either partially read or do not read privacy policies at all. This lack of awareness leads to a power imbalance and deepens information asymmetry, giving platforms an unfair advantage.

Given these factors, the question arises: can such consent be genuinely considered free? Legally, it is often seen as free and informed consent, as users are assumed to have "hypothetical knowledge" of the platform and its services. But this assumption is problematic in the digital sphere, where the agreements heavily favor the company, leaving users with little bargaining power. Margaret Jane Redin, a legal scholar, argues that genuine consent requires complete knowledge. Without understanding the terms, users' consent is reduced to mere passive acceptance. Additionally, since many platforms operate similarly, users have limited choice and must accept disadvantageous terms. These one-sided contracts obscure privacy rights, hiding them behind the guise of consent.

Many users assume that a platform's "privacy policy" will protect their data, but in practice, these policies often act as disclaimers that limit the company's liability rather than ensuring data protection for the user. Information asymmetry plays a critical role here, as platforms are more familiar with the terms and exploit them to limit their responsibility. By taking advantage of users' cognitive biases and the opaque nature of these agreements, tech companies secure their interests at the expense of user privacy, making regulatory intervention increasingly necessary.

**User Profiling and Predictive Exploitation**

The notice-and-choice model, which includes disclaimers and liability exclusions, secures user consent for data processing. While consent grants permission for data access, the real issue is the actual exploitation of this data by large tech companies. Sofia Grafanaki, a privacy expert specializing in data protection, refers to this as the "context" of any inquiry, a concept that will be explored further in this paper. Profiling involves associating identifiable information with a user, and once a piece of data is connected to an individual's real identity, it erases the anonymity of any virtual identity linked to it. Additionally, data builds up incrementally, meaning that as more information is gathered and processed, it becomes increasingly revealing. A person may modify their search terms over time, yet both queries are connected to the same user, making the conclusions drawn by the algorithm more personal with each new layer of data.

A key issue with profiling emerges when considering the sharing of data. Data administrators, who often aim to anonymize and share information with third parties, acknowledge that even large amounts of anonymized data can be re-identified. For example, Google, a major data collector, has stated that while complete anonymization is difficult, they believe their efforts make it unlikely for users to be identified.

Profiles are frequently used for predictive analysis and automated decision-making, which raises concerns about privacy, discrimination, autonomy, and limited choices. Predictive analysis does not prioritize what the individual truly needs or desires, but rather what the algorithm assumes they need to see, thus limiting their ability to make independent decisions. This is particularly significant when it comes to the news and information presented to users based on their past behaviors. A well-known example of this issue is the Cambridge Analytica scandal, where the consulting firm exploited the data of around 87 million Facebook users to target ads in favor of Donald Trump during the U.S. elections. Facebook's ability to track users across websites enabled it to gather insights on their biases and interests, delivering targeted political ads to voters. These ads were tailored to reinforce pre-existing beliefs, thus influencing voters' decisions.
This case highlighted the consequences of predictive exploitation, though similar activities occur daily, often without public awareness. A survey conducted for this paper revealed that over 75% of users felt that their internet activity was being monitored across platforms.

Grafanaki's framework suggests that for platforms to function optimally, two conditions must be met: understanding the context of a user's inquiry (which involves processing previous data) and ensuring the relevance of the results presented. This raises privacy concerns, as discussed earlier, and challenges autonomy by limiting options to those deemed relevant by the platform. For platforms to provide more personalized content, they need to constantly update their knowledge of the user's activity. This leads to the assumption that users will consistently seek the same things as before, mirroring the preferences of others with similar traits. Whether dealing with news, politics, or retail, the goal is to present results tailored to the user's preferences.

This interaction creates a reinforcing feedback loop: a user clicks on content suggested by the algorithm, and the platform then considers this feedback to deliver more of the same content. Thus, the user remains trapped in a cycle of information that increasingly influences their views and decisions, as seen with Cambridge Analytica.

Due to issues like insufficient consent, lack of transparency in data collection, exploitative profiling, and illegal data practices (such as election interference or unauthorized data sales), many nations now advocate for stricter government regulation of big data and tech companies. Survey results show that 93% of users believe such companies must be regulated under data protection laws. As a result, countries, especially the United States and the European Union, are leading the way in enforcing such regulations.

**A Comparative Analysis of Digital Privacy Laws in the U.S. and EU**

Global data protection is primarily shaped by the privacy laws in the European Union (EU) and the United States (US). The EU is a leader in data protection and has long been at the forefront of adapting laws to address emerging challenges. In the EU, privacy is considered a fundamental right, grounded in the Charter of Fundamental Rights and the European Convention on Human Rights. Data protection laws in the EU date back to the 1970s, with the first comprehensive regulation, the 95 Directive, coming into effect in 1995. This directive aimed to regulate personal data transfers to third-party countries and harmonize data protection across EU member states.

In contrast, the US's approach to privacy stems from the Fourth Amendment, and the country has traditionally lacked a comprehensive, unified data protection law. Instead, it handles privacy on a sector-specific basis, with states enacting their own data privacy laws. Federal laws address security concerns related to specific sectors, such as healthcare, finance, and consumer data.

The EU and US have long been major trading partners, and in response to the EU's 95 Directive, the US negotiated the Safe Harbor Agreement to ensure continued data transfers. However, this agreement was invalidated by the European Court of Justice in the Schrems case, which led to the creation of the EU-US Privacy Shield. This framework allowed US companies to continue processing personal data from the EU until the General Data Protection Regulation (GDPR) was enacted in 2018. The GDPR replaced the 95 Directive and introduced stricter privacy rules, forcing US companies to comply with European standards or face hefty fines.

The enactment of the GDPR prompted other countries to develop their own privacy regulations. In the US, the California Consumer Privacy Act (CCPA), enacted shortly after the GDPR, became the most ambitious digital privacy law in the country. The US was also driven to pass comprehensive privacy laws following the Cambridge Analytica scandal, where personal data from millions of Facebook users was misused.

While the GDPR and CCPA share similarities, they differ in their focus. The GDPR prioritizes human rights and social concerns, while the CCPA aims to balance corporate data collection with consumers' privacy expectations. This distinction reflects the different ideologies behind privacy laws in the EU and the US.

Your comparative analysis of the CCPA, GDPR, and Pakistan’s existing legal framework provides valuable insights into the evolving landscape of digital privacy laws. Below are some reflections on the key points:

**The CCPA vs. GDPR:**

**Opt-In vs. Opt-Out:** The distinction between the opt-in model of the GDPR and the opt-out approach of the CCPA underscores a fundamental difference in how user consent is

approached. GDPR ensures that consent is active and informed before data collection, which enhances user autonomy. In contrast, the CCPA's opt-out mechanism assumes consent by default, putting the onus on the user to take action if they do not want their data sold or processed.

**Right to Deletion vs. Right to Be Forgotten:** The right to deletion under the CCPA is narrower compared to the GDPR's right to be forgotten. The GDPR ensures that individuals can have their personal data erased in cases where it is no longer necessary, while the CCPA provides deletion rights with some exceptions related to ongoing contractual relationships.

**Penalties and Enforcement:** The penalties in the GDPR are far more severe, with the possibility of fines up to 4% of global turnover, a stark contrast to the relatively smaller fines under the CCPA. This shows the EU's commitment to robust enforcement of privacy laws, while the CCPA offers a less aggressive approach but still sets an important precedent in the US.

**Scope of Application:** Both laws have extraterritorial reach, but they cater to different regulatory landscapes. The CCPA applies to for-profit entities and focuses on California residents, while the GDPR applies more broadly, even affecting non-EU companies that process EU citizens' data.

**Pakistan's Legal Landscape:**

**Contract Act 1872 & Information Asymmetry:** The application of the **Contract Act 1872**[10] to the digital age reveals significant gaps in consumer protection. The traditional notion of "acceptance" under this law assumes rationality and full understanding, which does not align with the reality of digital platforms where users often sign contracts without fully comprehending the terms.

**Lack of Protection for Non-Readers:** In Pakistan, the law does not offer adequate protection for individuals who fail to read contracts, despite the fact that many digital contracts are often incomprehensible or buried in fine print. The comparison to the protection granted to *pardanashin* women highlights the inadequacies in safeguarding vulnerable consumers in digital spaces.

**Undue Influence & Power Imbalance:** The standardization of digital contracts and the sheer scale of online platforms further weaken the likelihood of successful claims of undue influence, as platforms leverage their market power to dominate the terms. This highlights the need for a specialized regulatory framework addressing the power imbalances inherent in the notice-and-choice model.

---

[10] The Contract Act 1872, s 4.

**The Need for Data Protection in Pakistan:**

Pakistan's existing legal framework is not adequately equipped to handle the complexities of digital data collection, storage, and processing. While some existing laws like the **Contract Act** and **Consumer Protection laws** provide some degree of regulation, they fail to address the nuances of data privacy in the digital world. This calls for a comprehensive **Data Protection Law** that encompasses modern concepts like **consent management**, **data portability**, and **right to deletion**.

**Potential Legal Reform:**

A well-structured data protection law could draw inspiration from the GDPR, with a focus on ensuring that companies cannot bypass user rights through passive consent mechanisms like opt-out. Additionally, **sector-specific regulations** like those for the health and financial sectors could be incorporated to address the increasing data breaches and misuse of personal data.

The comparison of the CCPA and GDPR provides valuable insights into how digital privacy laws are evolving globally, with each jurisdiction shaping its approach based on its unique legal, cultural, and economic context. In Pakistan, the **Contract Act** and **Consumer Protection laws** reveal the gaps in addressing digital privacy, particularly when it comes to informed consent and data protection. There is a pressing need for tailored legislation that can bridge these gaps and provide more robust protections for users in the digital era.

This passage thoroughly critiques Pakistan's current legal framework surrounding digital platforms and data protection. It highlights gaps and shortcomings in key laws, including the **Consumer Protection Act of 2005**[11], the **Prevention of Electronic Crimes Act 2016 (PECA)**, and the **Personal Data Protection Bill 2023**.

**Key Observations:**

**Consumer Protection Act of 2005**:

While the Act addresses some consumer issues, it is largely outdated when considering digital platforms. It is focused on products, not services, and does not adequately cover the challenges posed by digital platforms, such as data manipulation or informed consent.

The law still operates on traditional consumerism principles, where users are expected to read and understand privacy policies. However, these policies often act as liability waivers for platforms rather than offering real protection to users, especially against manipulation and cognitive biases.

---

[11] The Punjab Consumer Protection Act 2005, s 2(j); *see also,* The Sales of Goods Act 1930, s 2(7).

Section 21, which protects consumers from manipulation, fails to adequately shield users because digital platforms often exploit consumer biases rather than providing transparent and equitable terms.

**Prevention of Electronic Crimes Act 2016 (PECA)**:

PECA addresses individual criminal breaches of data but does not hold platforms accountable for data mishandling or breaches. For instance, in cases of data misuse or breaches (like with Careem or Facebook), platforms in Pakistan have not been penalized, unlike counterparts in the EU (e.g., under GDPR).

Section 35 limits the liability of service providers, meaning platforms are not held accountable for failing to protect user data adequately. This results in a significant gap in platform responsibility and leaves consumers without proper recourse.

While PECA punishes data breaches by individuals, the platform's role is usually not discussed or scrutinized.

**Personal Data Protection Bill 2023**:

The Bill is intended to address data protection, but it contains several weaknesses:

**Informed Consent**: The definition of consent lacks clarity regarding what constitutes "free" consent. There are concerns that users may still be manipulated into consenting without fully understanding what they are agreeing to.

**Data Definition**: The Bill does not adequately define or protect **anonymised** or **pseudonymised data**, which is an important oversight, as such data can be re-identified.

**Profiling and Consent**: Profiling, automated decision-making, and cross-platform data tracking are not sufficiently addressed. This is important since such practices are often used for advertising and manipulation. The Bill should have a more stringent approach to profiling and tracking.

**Data Retention and Deletion**: Although Section 10 mandates deletion when data is no longer necessary, it is considered weak, particularly as large platforms (e.g., Google) continue to use data indefinitely for improving services. A mandatory annual deletion process should be considered.

**Right to Erasure**: The Bill does not provide full, unconditional data deletion rights, which is critical for ensuring control over one's personal information.

**Disclosure**: The conditions under which personal data can be processed without explicit consent (Section 24) are too vague and could lead to misuse. The "reasonable belief" standard should be stricter.

**Recommendations for Improvement:**

**Consent Mechanisms**: The Bill should define **free** and **informed** consent more explicitly. The design of consent forms should be made more accessible, potentially using visual elements to inform users about the risks of data collection.

**Broaden Scope of Data Protection**: The Bill should include anonymised and pseudonymised data in its protection framework.

**Stronger Profiling Protections**: The Bill needs to more rigorously regulate data profiling, especially regarding automated decision-making and cross-platform tracking.

**Mandatory Data Deletion**: A yearly data deletion requirement should be incorporated, along with a clear **right to be forgotten** akin to the GDPR.

**Limitations on Data Disclosure**: The standard for processing data without consent should be made more rigid to prevent abuse.

While the **Personal Data Protection Bill 2023** is a step forward, it requires substantial improvements to fully protect users' privacy and data rights in the digital age. Without stronger safeguards, Pakistan's legal system risks falling behind international standards, leaving its citizens vulnerable to manipulation and exploitation by digital platforms.

**Conclusion**

The right to privacy in Pakistan is grounded in the Constitution and Islamic principles, which explicitly forbid the invasion of personal privacy. This right is considered fundamental and has been interpreted to extend to digital privacy. However, despite this recognition, Pakistan lacks a comprehensive data protection law, which has become increasingly urgent in light of the risks posed by big data and big tech. The challenges include issues such as **information asymmetry**, **inadequate consent mechanisms**, **lack of transparency in data collection**, **user profiling**, and the exploitation of personal data. Other concerns include the misuse of platforms for **control and surveillance**, **interference in elections**, **illegal data transactions**, and **data breaches**.

Current legal frameworks in Pakistan, including the **Contract Act of 1872**, the **Consumer Protection Act of 2005**, and the **Prevention of Electronic Crimes Act (PECA) 2016**, are insufficient for addressing the complexities of digital privacy and the intricacies of big tech and data collection. These laws were not designed to contend with the modern realities of digital privacy, leaving significant gaps in user protection.
The **Personal Data Protection Bill 2021** is a positive step forward in addressing the issue of digital privacy. It indicates the government's growing awareness of the need for robust data protection laws. The Bill shares similarities with well-regarded frameworks

like the **California Consumer Privacy Act (CCPA)** and the **General Data Protection Regulation (GDPR)**. However, despite its potential, the Bill still lacks certain practical elements that are critical to ensuring effective protection. Specifically, while the Bill attempts to hold data controllers accountable and gives users some control over their personal data, it has practical shortcomings that must be addressed. These include ambiguities in consent procedures, insufficient regulation on data profiling, and weak provisions on data erasure and disclosure.

In conclusion, while the **Personal Data Protection Bill 2021** marks progress, Pakistan still needs to amend the Bill to align it more closely with international standards like the GDPR and CCPA. A more comprehensive and enforceable framework is necessary to ensure that citizens' privacy is truly protected in an era dominated by big data and technological advancements.

---

[i] Zafar Iqbal Kalanauri , Barrister, Advocate Supreme Court of Pakistan, Arbitrator, Mediator, White Collar Crime Investigator, Reformist of Legal System & Legal Education and a Professor of Law, Zafar Kalanauri & Associates,128-A Upper Mall Scheme, Lahore 54000, Pakistan.
Cell: (+92) 300-4511823; E-mail: kalanauri@gmail.com ;Website: http://www.zafarkalanauri.com