Journal of Digital Media, Communication & Policy
Vol. 1, Issue 1, 2026

Vol. 1, Issue 1, pp. 35-47, 2026

Media Regulation and Platform Governance in Pakistan: Evaluating Policy Frameworks for Digital Rights and Privacy

Bilal Ahmad*^1

^1 Graduate, University of the Punjab
*Corresponding author: journals@isrnjournals.org

Abstract

The issue of social media misinformation poses a governance challenge to Kenya in the form of consumer trust, electoral integrity, platform engineering and constitutional rights. This paper discusses the nature of the development of misleading information in the context of the Kenyan digital media and considers the policy responses and the accountability of platforms. It relies on a critical narrative review of scholarly literature, Kenyan legal tools and institutional reports, as opposed to providing original field data. The discussion relates psychological accounts of misinformation to the political economy of digital sites and the multilingual population of Kenya. It claims that making a wide-ranging definition of falsehoods criminal is an unsatisfactory basis on information integrity, especially after the Court of Appeal ruled on false-publication offences in March 2026. A more justifiable solution is a combination of accurate legal safeguards, open platform procedures, responsible advertisement, free research, and easy corrections and long term media literacy. The article suggests an integrated system and allocates roles to governmental agencies, forums, newspaper and televisions and researchers and civil society without sacrificing privacy and civic engagement. Its major finding is that responsibility should be focused on the systems that enhance the negative information and give substantial solutions as well as work on enhancing personal judgment.

Key words: *Pakistan, media regulation, platform governance, digital rights, privacy, PECA*

PDF Download | Cite This | Share

Article History

Received: 24 June 2026 | Revised: 28 July 2026 | Accepted: 26 August 2026

1. Introduction

Digital media has transformed the way individuals in Pakistan obtain news, discuss political matters, communicate and conduct business privately. Social networks and messaging services provide the ability to publish without traditional newsroom gatekeepers, but they also disseminate harassment, false claims and personal information at a very high rate. The harms require governance to be responsive to, without jeopardizing the communication that promotes accountability and participation. The main dilemma facing Pakistan is how to increase regulatory intervention, and what protections come with it. This paper suggests that authentic platform regulation hinges on well-articulated authority, enforceable privacy assurances and reachable sanctions on harmful actions as well as improper restriction.

© 2026 The Authors | Published by ISRNJ

The regulation of media and governance of platforms are interrelated, though they are distinct. Licensed organisations, professional content and distribution infrastructure are generally the subject of broadcasting regulation. The rules, design options and institutional relationships which digital services structure communications and process user information are part of platform governance. Gorwa (2019) finds these associations between governments, companies, users and other actors. The way in which a television regulator operates can thus not be replicated to the social media without adapting. Platforms bring together a variety of speakers, suggest content and gather behavioural information, frequently internationally. Their regulation needs concern both to the private rulemaking and the technical architecture along with the behaviour of individual publishers.

Digital rights offer evaluative basis. These include the right to express, privacy, information access, equality and fair procedure since these rights are carried out using digital systems. Article 14, expression and press freedom within certain restrictions as mentioned in Article 19, and access to information in Article 19A of the Constitution of the Islamic Republic of Pakistan (1973) safeguards human dignity and privacy of the home. These provisions cannot be seen as equal to a comprehensive data protection regime that is enacted. However, they lay down critical constitutional interests against which regulatory practices can be scrutinized, as well as international human rights responsibilities that can be considered.

This article poses the question of whether the regulatory powers of Pakistan is accompanied by independent checks against these powers, responsible data processing and available remedies. The literature is reviewed, methodology elaborated, findings given and recommendations developed in the following sections.

Literature review

Platform power, information privacy and digital intervention are linked to the literature. Implementation and impact still need to be determined using country-specific evidence. Napoli (2019) places the social media regulation in the context of the general governance of the common good and the democratic role of communication.

Privacy encompasses more than keeping secret or preventing hacking. According to Nissenbaum (2004), privacy can be understood in terms of contextual integrity: the flow of information may be inappropriate when the norms and purposes of the environment where information was provided are not taken into consideration. A phone number, which is provided to receive a service is not necessarily a good material in political targeting. In the same manner, information disclosed to a small group would be detrimental when it is revealed to a larger audience. Solove (2006) singles out several privacy issues, such as aggregation, surveillance and disclosure. These views enable the article to assess the use of data without diminishing protection to whether the information was originally confidential.

The analysis is also based on literature about the topic of private power. The platforms make the masses communicate in a certain way due to contractual guidelines, advertising mechanisms and visibility decisions. Klonick (2018) looks at their position as regulators of online speech, whereas Cohen (2019) relates informational capitalism to the transformation of the legal and institutional power. These descriptions imply that both state action and corporate freedom can pose a risk to rights when not sufficiently limited. A rights-respecting framework should ensure that both government and companies are held accountable in regard to the consequences of their decisions. Pasquale (2015) goes further to justify why obaque institutional systems need to be checked by outsiders. Government approval or acceptance of a platform is not a statement that a practice is proportionate, fair or protective of users.

Platforms play a role in governing by content rules and design choices even where it is run under national legislation. Gillespie (2018) illustrates moderation as the key feature of platform organisation, and van Dijck et al. (2018) relate platform systems and the values of the population. This should not be limited to responding to state requests in Pakistan. Businesses should look into the impact of recommendations,

monetisation and reporting solutions on users. A service can agree to a takedown order but can still fail to safeguard privacy and offer fair appeals. Legal compliance is a significant minimum, but not the full scope of the duties of powerful communication infrastructure.

An efficient practice separates the duty of hosting, amplification and commercial promotion. A platform will not fact-check every statement prior to its publication, but it will make consequential decisions on what is recommended or paid reach. Helberger (2019) attributes a democratic goal to news recommendation, and the idea is that the ranking systems should be evaluated based on more than engagement. Such questions as the visibility of good reporting, exposure to recurrent abuse and the ability to experience a variety of information are relevant to Pakistani audiences. The assessment should look at real results and user options, and not assume that a single homogeneous ranking model will fit all communities or communication objectives.

Linguistic and cultural competence is a requirement of content moderation. Pakistani communication incorporates Urdu, English and many regional languages, and mixed scripts and informal transliteration. Threats may be relative and a satire may be misinterpreted by literal translation. Gorwa et al. (2020) elaborate on technical and political constraints of automated moderation. Platforms ought to analyze mistakes in applicable languages and formats, such as audio and video. Human escalation is particularly important for consequential decisions. Offering a locally informed process does not ensure the correctness, but contextual interpretation becomes more likely and offers a path to rectifying automated errors.

Moderators working conditions are included in that process. Roberts (2019) reveals the labour behind commercial content review, such as viewing upsetting content or organisational limitations. Firms ought to train, offer workload and support to the employees who moderate harmful material. Assessment should also safeguard assessors against political intrigue and retribution. The policies must be informed by the Pakistani expertise, but no specific reviewer is supposed to solve the complex issues in the country on his or her own. Escalation procedures are clear and policy standards are documented, which aid in maintaining consistency. Enhanced worker support not only meets the labour interests but also the quality of protection to the users.

The influence of perceived monitoring may not be limited to interception of a certain message. Penney (2016) provides evidence that is consistent with the chilling effects on information seeking after the release of surveillance, whereas Stoycheff (2016) investigates the perceptions of surveillance and the readiness to voice minority opinions. Both studies do not estimate effects in Pakistan. They do, however, provide plausible mechanisms which need local investigation. When they think it is traceable, people might not contact the sources, research on sensitive issues or complain about dissatisfaction. Privacy framework safeguards such social functions or even personal confidentiality, and therefore, the accountability of surveillance applies both to journalism and the civic life.

Routine commercial processing is also related to privacy protection. Platforms make inferences and tailor feeds and sell access to users on the basis of information that the latter may not comprehend entirely. Acquisti et al. (2015) discuss behavioural boundaries in making privacy choices, disproving the premise that consent to a notice is always a strong indication of an informed decision. Nissenbaum (2010) also focuses his attention on the suitability of information flows. In the case of Pakistan, a strong framework would entail clear explanations, restrictions on secondary use and controls that are available. Consent should not be turned into a process whereby organisations transfer all the burdens to those who do not have much bargaining power in reality.

Profiling raises other equality issues. According to Barocas and Selbst (2016), even in the absence of explicitly discriminatory variables, data-driven systems can generate disparate effects. Inferred attributes can have an effect on access to advertising, exposure to content or automated enforcement, in platform environments. Pakistan-specific testing needs to look at whether a language, location or other proxies have

a systematic disadvantage to some users. This should be backed by relevant evidence and protection, and not the assumption that all algorithms are discriminatory. Impact assessments, limited retention, documented testing can be used as privacy and equality evaluation. Consequential error should be remedied by placing users in wrong categories or placing them out based on unfairness.

Of particular concern is gendered harm, which is subject to unequal social impacts through online exposure. A study of women and NGO employees in India, Pakistan and Bangladesh, by Sambasivan et al. (2019) reported abuse such as impersonation, stalking and personal-content leakages. Their local qualitative results must not be considered as a national prevalence estimate. They, however, demonstrate why invasions of privacy cannot be considered in terms of financial loss alone. Reputation damage and offline danger as well as threats demand responsive support. The framework of Pakistan needs to offer confidential complaints, prompt response to non-consent exposure, trained staff and does not use procedures that expose the complainants to further disclosure or blame.

The idea of cooperative governance provides an opportunity to share responsibilities without blurring them. According to Helberger et al. (2018), the public values demand communication between platforms, users and institutions. Pakistan can use this principle by conducting its own research, by having civil society involvement and agency directives. Cooperation does not imply that companies silently consent to put restrictive rules with authorities, or delegate unpaid crisis work to local organisations. Contracts must have published goals, funding revelation and examination. All actors should be accountable regarding their own choices, so collective participation is an addition to, not a substitute of corporate responsibility and social institutional accountability.

Methodology

This paper has a qualitative documentary design with a critical literature review of the literature and analysis of the legal policy. It bases its analysis on the policy framework, encompassing constitutional interests, statutory powers, and proposed privacy safeguards and platform responsibility mechanisms. The corpus used in this paper is the 42 sources that will be referenced in the article: scholarly publications, official documents related to the law and policy, and reports of institutions pertinent to Pakistan. Conceptual relevance, direct country relevance, and utility in assessing governance alternatives were some of the factors used in selection. This is not a systematic review that purports to be exhaustive. There was no interviewing, survey or original measurements.

The analysis systematises the material based on six assessment criteria: legal accuracy, institutional autonomy, proportionality, protection of privacy, procedural fairness and inclusion. It juxtaposes the distribution of regulatory authority and the safeguards and remedies that come with it. Formal authority is defined by legal instruments, formal explanations are found in academic literature, attributable reporting of implementation and disputed practices are found in institutional reports. Provisions enacted are differentiated by proposals, statutory design by demonstrated operation. The sources are up to date to September 2026. International studies provide information to inform interpretation, but do not determine Pakistan-specific causal effects, whereas qualitative and advocacy reports do not determine the national prevalence. The conclusions are thus an interpretive policy evaluation the findings of which are confined to the documentary evidence.

Findings

Regulatory architecture and institutional safeguards

The institutional framework in Pakistan formed the regulatory environment based on institutions that had various purposes. PEMRA bases its regulation of the private electronic media, the broadcast and distribution activities on the Pakistan Electronic Media Regulatory Authority Ordinance, 2002. The telecommunications

regulating is under a different institutional and legislative framework. Investigative and online-content functions are added to cybercrime law. Such a multifaceted development may create ambiguity in cases where the same news story is represented in television, a media house web site and a social media. A good assessment should determine who is exercising a certain power and by what authority instead of defining all intervention as media regulation.

PECA or the Prevention of Electronic Crimes Act, 2016, provides a legal framework of electronic crimes, such as unauthorized access and behavior that has an impact on personal safety. Its original section 37 also provided a route for online-content removal or blocking. This mix is important as investigating a cybercrime and policing the general discourse involve various authorities and protections. Specific action against fraud can safeguard the users, whereas general action into legitimate argument can inhibit them. PECA ought to be considered accordingly on a provision by provision basis. Availability of the needed cybercrime protections does not address the issue related to the scope of other regulatory authorities or to their management.

The Removal and Blocking of Unlawful Online Content Rules, 2021 codified processes and requirements relating to the previous content-control system. The rules are approved legislation by the Ministry of Information Technology and Telecommunication. Caution should be observed in their relation to the later amendments: historical commitments must not be given as a whole and unalterable history of the system in existence. The real question of evaluation is whether introduction of rules sufficiently restricts administrative discretion and maintains substantive control. Protection is not simply created by the use of procedural terms, but rather by what is available to reasons, to appeal decisions and remedies, how the safeguards are applied in practice.

Another significant statutory amendment was the publication of the Prevention of Electronic Crimes (Amendment) Act, 2025, on 29 January 2025. It establishes a Social Media Protection and Regulatory Authority, a complaints mechanism and a Social Media Protection Tribunal, and includes national cyberspace crimes investigation agency in PECA investigations. The amendment also has transitional provisions. Such are characteristics of the institutional design enacted; their presence does not reveal that all bodies and remedies work well. Implementation has to be assessed using more evidence regarding appointments, staffing, procedures and decisions and does not presume institutional capacity based on legislative language.

The amendment adds section 26A that deals with intentional spreading of information that is known to be false or fake and has a high likelihood of causing certain disturbances within the population. The highest penalty is a three-year jail term, two million rupees fine or both (Prevention of Electronic Crimes [Amendment] Act, 2025). Mental and consequence-related elements are also included, which is pertinent to the analysis of law. Nevertheless, the interpretation is vital: it is unclear what would be considered disorder or unrest, and it may influence the attitude to urgent reporting and provocative statements. The policy issue is application reliably separates harmful deception and legitimate participation.

The statutory design offers platform enlistment and instructions regarding unlawful or offensive content as well, and can be appealed to by the tribunal and further to the Supreme Court (Prevention of Electronic Crimes [Amendment] Act, 2025). This article considers those mechanisms as issues that need to be assessed and not as an indication of adequate accountability. Formal appeal pathway might be not easily applicable where a person does not have legal representation, where a person suffers an immediate loss of access or fails to receive a decisive explanation. Even practical remedies are based on cost, timing and independence. These issues are especially relevant to the common users and small publishers who have little administrative resources.

These reforms have been questioned by local organisations. The Human Rights Commission of Pakistan (2025) demanded the repeal of the amendment, and Digital Rights Foundation (2025) documented the issues of legislation impacting digital expression. The organisations should see these interventions as an assessment and not a judicial determination. They still show that regulatory legitimacy is still a contentious issue among concerned parties. Such objections need to be included in an inclusive policy process by involving the substance of these objections such as the interaction between the safety of the people, institutional authority and freedom of expression of powerful actors. The process of consultation is meaningful when it can have an impact on text and implementation.

The law of privacy is on another course. Personal Data Protection Bill, 2023 is still a working document in the official text analyzed in this paper; the article does not specify how the ministry proposes to commission or bind itself as a nationwide regime. This is a critical difference since draft rights are incapable of providing the same remedies as enforceable legislation. The current constitutional rights and industry safeguards are not irrelevant and may not provide blanket restrictions on collection, profiling and subsequent transfer. The issue of privacy reform then should be evaluated independently of the increase in cybercrime and content-regulation authority.

The National Data Governance Policy, 2026 proposed has another strand that relates to government data. According to Pakistan Digital Authority (2026), the policy is defined as a proposed framework designed by the ministry, and its site documents the end of the stakeholder feedback. The data-governance policy will be able to enhance stewardship and sharing, but it cannot be supposed that it will provide all the protections of a personal-data statute. To make administrative data more useful, there must be restrictions on identifiable information, accountability and means of redress in case of its abuse. The article thus assesses this initiative as a new policy trend, not stating legislative implementation or even a well-established implementation.

Combined, the arrangements bring about an asymmetry: there are elaborate plans on how to intervene on the communication, yet, overall protection of privacy is still floated via the reviewed sources. It is a critical evaluation of the architecture, not to say that all other existing institutions do not care about privacy. The imbalance however influences policy priorities. Further content-control capability can broaden the implications of gathering and connecting data on users. The trust of the people lies in the ability to balance that capacity with limits that are enforceable and to be checked by an independent authority. Regulatory coherence implies matching goals and protection, and not merely an addition of an extra authority to an already stratified system.

Expression privacy and access to remedies

The initial evaluative test is legal precision. The prohibited conduct should be identified through restrictions and the evidence required to prove it. General ideas may include real danger as well as mere discord, satire and false reporting. According to the United Nations Human Rights Committee (2011), any restrictions on expression should meet the standards of legality, necessity and proportionality. This framework applied to Pakistan helps to make a cautious distinction between cyberstalking, impersonation and incitement and criticism. Authorities should tell the public what interest is at risk and why the intervention chosen is reasonable. The use of security or public order in the absence of an evaluable relationship to the behavior undermines accountability.

Accuracy should be applied to enforcement practice. A rule may include restrictive language but be interpreted broadly where investigators or administrators can use the criticism as an indication of ill-will. Statutory reform should therefore be accompanied by training, reasoned decision making and independent review. There is necessarily uncertainty in reporting in the developing events, and the errors can be made without intentional misrepresentation. The article suggests safeguarding good-faith public-interest reporting by means of standards, which involve close analysis of evidence and context. They are proposals of reform

and not assertions concerning current exemptions. The idea is to minimize arbitrary intervention but maintain relative reactions to well-defined harmful behavior.

The second test is a test of the connection between limiting speech and communal safety. Targeted attacks and revealing intimate content, as well as fraud, can inflict severe damage and warrant effective protection. Nevertheless, the extent of damage does not proportion all the possible measures. The deleting of one particular illegal upload is not the same as blocking a whole site of news, business and confidential communication. DeNardis (2014) demonstrates that the domination of the infrastructure may turn into political control. Network access decisions in Pakistan should be considered to have collateral consequences, duration, geographic coverage as well as the existence of less restrictive options.

In May 2025, Freedom House (2025) recorded disruption of connectivity, and reported that X was made available in May 2025, following restrictions since February 2024. This dated record will not allow the previous limitation to be characterized as constantly up-to-date. It also shows how access conditions should be monitored separately. An interruption can include deliberate blocking, technical failure or otherwise and analysis cannot be made on attribution basis and should not be attributed without evidence. The users also have less access irrespective of the immediate explanation. Public discussion of network interference would be more precise and responsible with transparent notices and published authorisations, where applicable, and independent technical assessment.

A similar, yet different, set of concerns pertains to surveillance. In a report by Amnesty International (2025), it was claimed that a large censorship and surveillance system was in place in Pakistan and that international suppliers were involved. The findings of Amnesty should be assigned to them, and evaluated using the evidence used in the report, instead of being replicated as a separately measured national figure. The implication of governance is that there should be scrutiny of procurement and technical deployment. Legal investigative equipment may be used to facilitate over-monitoring in cases where there is poor authorisation, access controls and supervision. The role of suppliers and local institutional protection is hence a complementary aspect of privacy protection.

There should be an alignment between data collection purposes. An organisation must explain the reasons why this or that category is required, who is allowed to access it and how long it will be stored. This will minimize the impact of misuse as well as security failure. The taxonomy by Solove (2006) reveals why the issue of privacy risk cannot be resolved by only preventing unauthorised disclosure. Combining valid entries may reveal a set of relationships and behaviours unintended. Reuse and linkage, as well as collection, should be proposed as Pakistani privacy legislation. In order to ensure that protection is credible, there should be meaningful obligations to be undertaken by public bodies together with the private companies.

Security and privacy should also be differentiated. With very robust access controls, a database may be resistant to attacks by outsiders but excessively collected data or improperly used internally will remain untouched. On the other hand, restricting the collection without proper security will reveal the rest of the information. Cohen (2019) links such institutional options with informational power at large, whereas Lessig (2006) focuses on the way architecture influences behaviour. Good Pakistani governance must thus entail technical security and warranted processing. Purpose limits and independent oversight should be used with encryption, audit logs and access restrictions. The protection is also undermined when an organisation relies on cybersecurity claims to escape the examination of its own data practices.

The last test of practical protection is the availability of remedies. A legal right will not mean much to a user who is not able to recognize the organisation that bears the liability and can file a complaint or comprehend a decision. Correction, restoration, deletion where warranted, compensation where warranted by law and investigation of recurrent failures should be remedies. Their rights also need protection against competing rights. The decision on an erasure request in connection with public-interest reporting should not be

determined by the choice of the requesting party, but a victim of intimate-image abuse should not be subjected to undue delay. Independent assessment should take into account context and be reasoned and fairness should not be seen as an empty promise.

Platform responsibilities and governance gaps

Decisions should be described in a transparent form that can be evaluated by the users and independent observers. Businesses would be able to share country-wide legal requests, types of enforcement, time and appeal rates as well as safeguard confidential data. The article suggests these disclosures as accountability standards as opposed to claiming that they are available across services. Numbers of raw removals are not adequate as they may indicate varying degrees of negative activity, detection or over-enforcement. Estimated exposure precedence and the number of reversals should be a contextual measure. To identify real improvement, methodological explanations are required to differentiate between the new definition and counting practices.

Separate reporting is required on government requests. A platform must document the requesting authority, purported legal basis and extent of the demand, under a strictly limited confidentiality. Where requests have impacts on such areas as reporting on the public interest or personal information, independent review should be possible. According to the United Nations Office of the High Commissioner of Human Rights (2011), business responsibility is to respect human rights by performing due diligence and remediation. In the case of Pakistan, it is a duty to evaluate plausible effects, not to assume that all official requests are legitimate by default. There are also internal escalation processes required in the companies where conflicts arise between demands and rights commitments or other relevant obligations.

Any substantial restriction should be accompanied by procedural fairness. Users should have an explanation of the appropriate rule that makes sense, a chance to give context and an appeal that does not merely recreate the original automated determination. According to Klonick (2018), there are processes that regulate the decisions to use private speech. In the case of journalists and creators, the long delay in restoring can have permanent effects, even in situations where a company can confess its mistake later. The platforms must then focus on cases that are time-sensitive and clarify on remedies of wrongful removal. Fairness is also extended to complainants: it is not fair to dismiss a report without having good reasons and leave the victims without any opportunity to receive protection and know what evidence is lacking.

Privacy by design offers a similar set of obligations. The default settings can limit unwarranted exposure, display audience boundaries, and discourage collection that is not related to a service. Cavoukian (2011) establishes privacy by design principles, and Acquisti et al. (2015) explain the impact of interfaces on the decisions of users. The controls that Pakistani users should be provided with must be comprehensible in terms of both the language and the digital literacy level. A privacy notice is no replacement of an interface that promotes such widespread disclosure or makes it hard to withdraw. Organisations must put controls into test under normal usage and whether more secure environments maintain a reasonable access to important functions.

Privacy is related to accountability of advertising. Political and issue advertising also has the capability of reaching audiences based on inferred attributes without disclosing sponsorship. The suggested solution is to verify the advertisers, archives that are searchable and restrictions on the use of sensitive data. Such measures are supposed to be developed without the establishment of redundant databases of regular users. Yeung (2018) discusses regulatory implications of the algorithmic systems, which is why the focus on understanding the way in which behavioural influence can be used is justified. Researchers in Pakistan must have some evidence on targeting practices before they claim to have certain effects on the electoral process. However, even in those cases when causal estimates of persuasion are not clear, clarity in sponsorship and processing can help to decrease the levels of opacities.

Platform obligations should not require surveillance as the regular method of enhancing safety. Public identity disclosure will reveal vulnerable speakers and private messages will be compromised. Deibert (2019) talks about the negative elements of the social media ecosystem, whereas Mueller (2017) talks about the implications of the nationally divided governance of the internet. Such options are user-controlled reporting, better restricted preservation requests and enhanced safeguards against mass abuse. Transparency to the public and private communication can exist. It is what information a particular purpose needs, what protection, not whether companies can fully expose all users to authorities.

Conclusion and recommendations

The digital governance of Pakistan needs to have a better linkage between protection and regulatory power. The framework under review has both valid cybercrime goals and disputed speech regulation and ambiguous issues concerning total privacy protection. Reform must narrow state action, make companies responsible and remedies accessible across linguistic and social boundaries. Privacy safeguarding should be extended to common commercial handling and surveillance and safety to individuals under gendered or targeting violence. The ability of users to communicate, to get protection, and to challenge consequential decisions will be what makes a credible system. The institutional expansion per se cannot provide those results without independence, evidence and prolonged public examination.

The first area of reform is to separate the protection of cybercrime with the extensive regulation of the discussion. Pakistan requires efficient feedback to fraud, stalking, threats and non-consensual exposure, as well as evident boundaries on restrictions of legal expression. The statutory review ought to challenge the sufficiency of the precision of every offence and the adequacy of its punitive measures to demonstrate harm. Decisions on content must be documented with reasons which can be disputed. The article suggests that contested speech provisions should be reviewed using constitutional and international criteria, but that a narrowly-tailored protection against actual abuse should be maintained. The aim is a more credible system of complainants as well as speakers.

Institutional independence is the second priority. Undue influence can be minimized by means of public appointment procedures, safeguarded terms, conflict-of-interest regulations and transparent budgets. Regulators are recommended to make their decisions and enforcement priorities public, effective to reasonable privacy constraints. Independent review should be cost effective and be able to provide interim relief at the right time when needed. These suggestions are about the quality of institutional design, and do not presuppose that the establishment of a tribunal or an authority will automatically bring about independence. Courts and civil society as well as parliament should be in a position to scrutinize the usage of powers. Oversight proves to be believable when it can spot and correct failures by strong institutions.

The third priority is the overall personal-data protection. Accountable processing should be defined by legislation, enforced individual rights and independent control should be provided. The key requirements ought to include purpose limitation, proportionate collection, security, retention and controlled transfers. Public-sector exemptions must be tightly justified and monitored to prevent the most far-reaching processing to be beyond question. The draft framework offers a platform on debate, yet enacted protection should be evaluated via final text and implementation. The General Data Protection Regulation of the European Union (European Parliament and Council of the European Union, 2016) can serve as acomparative source, not an example that Pakistan should follow without looking at its institutions and administrative capacity.

Fourth-priority is about authorisation of surveillance and procurement. Intrusive measures must demand the stated purpose, its independent review, and time restriction and access. Logs should be secure and audit procedures and retention rules must prevent unrelated reuse by operators. Procurement ought to evaluate the capability of suppliers to uphold the right human rights due diligence. The United Nations Office of the High Commissioner of Human Rights (2011) offers principles applicable to business behaviour, whereas

the inquiry of Amnesty International (2025) offers Pakistan-related arguments to study. Reform must take the form of demonstrable protection and solutions as opposed to promises that monitoring equipment will never be misused.

The fifth priority is a platform accountability framework that focuses on processes and outcomes. An analogous example of transparency and systemic-risk responsibilities is offered by the Digital Services Act (European Parliament and Council of the European Union, 2022), whereas UNESCO (2023) suggests the principles of governance associated with expression and participation. Pakistan ought to emulate practical features by consulting the population and evaluating them. First-time requirements might emphasize the establishment of clear channels of complaints, disclosure of advertising, reporting of local-language requests and appeals. The requirements must be risk and scale-based. A system that has complicated reporting with little or no action taken by it might be favourable to large organizations with minimal effect on protection to normal users.

Implementation needs sequencing and resources. The first step must map agency roles, develop public baselines, consult journalists, afflicted communities, businesses and technical professionals. The second step might be the pilot complaint standards, privacy tests and open reporting plans. Publication evaluation should be followed by expansion. Financing should be directed towards trained personnel and services and not just establishment of the organisation. Smaller publishers and businesses might need more practical advice on data duties, whereas bigger organisations should exhibit greater compliance ability. Clear responsibility will eliminate situations when each institution will consider the failures as the problem of another body.

The assessment should be based on the outcome of rights. The indicators of relevance are the response time to complaints, post-wrongful-restriction restoration, access to reasons, data breach, and proven recurrence of abuse and availability of privacy remedies. Studies must also be conducted on the possibility of interventions discouraging legitimate participation or putting complainants at further risk. The technical analysis of censorship in Pakistan by Nabi (2013) reflects the importance of measurement even though no description is done concerning existing infrastructure. Legal analysis can be supplemented with updated research on the network, user interviews and well-planned surveys. Publicized approaches and uncertainties would enhance the validity of results and correction of the policy would be achievable.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Amnesty International. (2025). *Pakistan: Shadows of control: Censorship and mass surveillance in Pakistan* (ASA 33/0206/2025). https://www.amnesty.org/en/documents/asa33/0206/2025/en/

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732. https://doi.org/10.15779/Z38BG31

Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/sites/default/files/legacy/2018/01/pbd.pdf

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press. https://doi.org/10.1093/oso/9780190246693.001.0001

Constitution of the Islamic Republic of Pakistan, 1973 (Pakistan). https://www.na.gov.pk/en/downloads.php

Deibert, R. J. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy, 30*(1), 25–39. https://doi.org/10.1353/jod.2019.0002

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Digital Rights Foundation. (2025, February 26). *Digital Rights Foundation study sheds lights on repressive digital expression legislation, including PECA*. https://digitalrightsfoundation.pk/6547-2/

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

European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union, L 277*, 1–102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Freedom House. (2025). *Pakistan: Freedom on the Net 2025*. https://freedomhouse.org/country/pakistan/freedom-net/2025

Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society, 22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society, 7*(1), 1–15. https://doi.org/10.1177/2053951719897945

Helberger, N. (2019). On the democratic role of news recommenders. *Digital Journalism, 7*(8), 993–1012. https://doi.org/10.1080/21670811.2019.1623700

Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society, 34*(1), 1–14. https://doi.org/10.1080/01972243.2017.1391913

Human Rights Commission of Pakistan. (2025, May 29). *HRCP calls for repeal of PECA (Amendment) Act*. https://hrcp-web.org/hrcpweb/hrcp-calls-for-repeal-of-peca-amendment-act/

Klonick, K. (2018). The new governors: The people, rules, and processes governing online speech. *Harvard Law Review, 131*(6), 1598–1670. https://harvardlawreview.org/print/vol-131/the-new-governors-the-people-rules-and-processes-governing-online-speech/

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Ministry of Information Technology and Telecommunication. (2023). *Draft of the Personal Data Protection Bill, 2023*. https://www.moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

Mueller, M. (2017). *Will the internet fragment? Sovereignty, globalization and cyberspace*. Polity Press.

Nabi, Z. (2013). The anatomy of web censorship in Pakistan. In *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13)*. USENIX Association. https://www.usenix.org/conference/foci13/workshop-program/presentation/nabi

Napoli, P. M. (2019). *Social media and the public interest: Media regulation in the disinformation age*. Columbia University Press.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Pakistan Digital Authority. (2026). *Pakistan Digital Authority to oversee the country's first National Data Governance Policy*. https://www.pda.gov.pk/press-details.php?id=data-governance-policy

Pakistan Electronic Media Regulatory Authority Ordinance, No. XIII of 2002 (Pakistan). https://pemra.gov.pk/assets/uploads/legal/Ordinance_2002.pdf

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117–182. https://btlj.org/data/articles2016/vol31/31_1/0117_0182_Penney_ChillingEffects_WEB.pdf

Prevention of Electronic Crimes Act, No. XL of 2016 (Pakistan). https://na.gov.pk/uploads/documents/1470910659_707.pdf

Prevention of Electronic Crimes (Amendment) Act, No. II of 2025 (Pakistan). https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf

Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, S.R.O. 1343(I)/2021 (Pakistan). https://www.moitt.gov.pk/Legislations

Roberts, S. T. (2019). *Behind the screen: Content moderation in the shadows of social media*. Yale University Press.

Sambasivan, N., Consolvo, S., Batool, A., Ahmed, N., Matthews, T., Thomas, K., Gaytán-Lugo, L. S., Nemer, D., Bursztein, E., & Churchill, E. (2019). "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Paper 2, pp. 1–14). Association for Computing Machinery. https://doi.org/10.1145/3290605.3300232

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564. https://doi.org/10.2307/40041279

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly, 93*(2), 296–311. https://doi.org/10.1177/1077699016630255

UNESCO. (2023). *Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach*. https://unesdoc.unesco.org/ark:/48223/pf0000387339

United Nations Human Rights Committee. (2011). *General comment No. 34: Article 19: Freedoms of opinion and expression* (CCPR/C/GC/34). https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

United Nations Office of the High Commissioner for Human Rights. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance, 12*(4), 505–523. https://doi.org/10.1111/rego.12158