CHARTING THE DIGITAL SURVEILLANCE MACHINERY OF PAKISTAN

MUSA SAEED | SAFA IMRAN

Musa Saeed is a fifth-year law student at the Lahore University of Management Sciences (LUMS), Pakistan. His primary interests include environmental law and climate change policy, and poverty law.

Safa Imran is a practising corporate lawyer based in Lahore. She graduated from the Lahore University of Management Sciences (LUMS) in 2023, and her academic interests lie in constitutional and human rights law and their evolution in an increasingly digitised world.

ABSTRACT

This article identifies the form of surveillance carried out and establishes the surveillance network of the Pakistani State. The modes through which this surveillance is carried out is meticulously analyzed, from phone and wire-tapping to surveilling data from service providers like telecom companies and internet service providers. All these State actions are legitimated through the country's legislative framework and this has had adverse implications for human rights and democratic processes. To combat this, there is a need for a consolidated national data protection act with stringent enforcement mechanisms that strike a balance between the right to privacy and necessary State surveillance for national security purposes, bringing Pakistan in line with its international human rights obligations.

KEYWORDS: Surveillance, surveillance network, privacy, PECA, PTA, FTA, GDPR, national security, state interests, international human rights law.

1. INTRODUCTION

Defining mass surveillance is complex. Simply put, it can be defined as a focused and systematic effort to obtain information for 'tactical and strategic purposes'.[1] In the age of surveillance, States have formulated a variety of modes of survey.[2] For the purposes of this article, the type of surveillance that best fits the phenomenon we are studying is dataveillance. Computer scientist Roger Clarke introduced the term 'dataveillance', which he defines

[1] SE Costanza 'Surveillance' in A. Javier Trevino (ed), *The Cambridge Handbook of Social Problems Volume 2* (Cambridge University Press 2018).
[2] Margaret Hu 'From the National Surveillance State to the Cybersurveillance State' (2017) 13 Ann. Rev. of L. & Soc. Sci. 161, 163.

as the 'systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'.[3] Dataveillance essentially 'provides a method by which all aspects of a person's life and identity may be transformed into digital data ready for analysis', and David Lyon elucidates upon 'the relationship between dataveillance and surveillance, explaining that dataveillance also automates surveillance'.[4]

The Pakistani State's digital surveillance methods can be seen as dataveillance as they heavily rely upon the data repositories from private service provider companies, CCTV cameras and social media companies in order to create their complete surveillance network. These repositories are large pools of digital data that are ready to be accessed and analyzed, and the system of collecting the data into the repository is entirely automated as computer systems receive and process this data continuously. In the effort to create and sustain this surveillance network, the right to privacy is disregarded by the State. This article shall demonstrate that Pakistan, as a surveillance State, is heavily invested in creating an extensive digital surveillance network through phone and wiretapping, partnerships with private service provider companies, access to CCTV footage and social media platform monitoring. The current legislative framework legitimates these State actions and provides them with a broad range of powers to carry out their surveillance methods, going against international obligations set for data protection and negatively impacting citizens. In the end, it will suggest how a comprehensive data protection bill can mitigate some issues and protect citizens' privacy.

1.1 The Constitutional Right to Privacy

In essence, privacy means freedom from unauthorised intrusion.[5] A foundational understanding of the right to privacy was first articulated in the 1890s, and it was described as the 'the right to be let alone'.[6] From that genesis

[3] ibid.
[4] ibid.
[5] Sabrina De Capitani Di Vimercati et al, 'Data Privacy: Definitions and Techniques' (2012) 20(6) International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 793 <https://doi.org/10.1142/S0218488512400247>.
[6] Samuel D. Warren and Louis D. Brandeis 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193 <https://www.jstor.org/stable/i256795>.

it has now developed to broadly be known as the freedom from any form of unwarranted interference or surveillance by any entity - State or private, and it is considered to be a fundamental right that is integral to human dignity and autonomy.[7] In Pakistan's Constitution, the right to privacy has been enshrined as a fundamental right under Article 14(1), which states that '[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable'.[8] The Supreme Court, in the seminal judgment of *Mohtarma Benazir Bhutto v President of Pakistan*[9] further enhanced this right by applying the protection of the term 'privacy' to all facets of the lives of Pakistani citizens and not just restricting it to the home by taking a literalist approach to the Constitution's text. Instead, the judgment noted that it refers to 'the privacy, which is sacred and secure like the privacy a person enjoys in his home.' A person is entitled to such privacy of home wherever he lives or works, inside the premises or in open land. A person's privacy cannot be intruded,[10] unless 'grave risk to the security of the country is involved'.[11] Therefore, it was upheld that the emphasis of the right to privacy was not limited only to a person's home but could be enjoyed wherever the person may be. It also affirmed that the inviolability of privacy is inextricably linked to the dignity of man:

> If a man is to preserve his dignity, if he is to live with honor and reputation, his privacy, whether in home or outside the home has to be saved from invasion and protected from illegal intrusion. The right conferred under Article 14 is not to any premises, home or office, but to the person, the man/woman wherever he/she may be.[12]

Extending this definition to the digital sphere, the privacy of communications entails the security and privacy of mail, email, telephones and forms of communications. Information privacy involves the establishment of rules

---

[7] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 ('ICCPR'), art 17(1).
[8] The Constitution of the Islamic Republic of Pakistan 1973 ('Constitution'), art 14.
[9] *Mohtarma Benazir Bhutto v President of Pakistan* (PLD 1988 SC 388).
[10] ibid [29].
[11] Divya Srinivasan and Gayatri Khandhadai 'Jurisprudence Shaping Digital Rights in South Asia' (2020) Association for Progressive Communications 32 <https://www.apc.org/en/pubs/jurisprudence-shaping-digital-rights-south-asia> accessed 29 December 2022.
[12] ibid 30.

governing the collection of handling of personal data such as credit information and medical records.[13]

Although the right to privacy has been expressly provided by the Constitution of this country and upheld by its Supreme Court, there is a severe lack of safeguards regarding privacy that does little to curb the dataveillance carried out by the State. To date, Pakistan lacks a consolidated national statute which governs the process of personal data collection, retention, processing, transfer, use and protection. Moreover, even concerning the laws regulating the right to communications privacy, the Pakistani government possesses overarching and opaque powers to surveil telephonic, email and other communications.

1.2 Pakistan's Surveillance Network

In Pakistan, Article 14(1) of the Constitution (right to privacy and dignity) contains a caveat: 'subject to law.'[14] This exception erodes the right to privacy entirely, as the country's current legislative framework allows the State to surveil and consequently discipline their citizens as extensively as they desire. While some data is obtained by consent, such as data obtained by social media and telecommunications companies, the law allows for data to be extracted and used in ways that the data subjects have no control over.

To understand the surveillance network, this section will be looking at various parts of the Prevention of Electronic Crimes Act, 2016 (PECA), the Punjab Safe Cities project, and other legislative provisions in relation to State control and national security, focusing on provisions laying down surveillance techniques.

The underlying theme behind the promulgation of the PECA was to 'keep a check on digital harassment, curb hate speech and control the proliferation

[13] David Banisar 'Privacy & Human Rights - An International Survey of Privacy Laws and Developments' (1999) 18 The John Marshall Journal of Computer and Information Law <https://www.researchgate.net/publication/242448871_Privacy_human_rights-an_international_survey_of_privacy_laws_and_developments>
[14] Constitution, art 14.

of extremist content.'[15] However, the Act has given 'ample leeway to the government to silence dissent'[16] through the broad powers it grants the State to access data through authorised agents appointed by the Federal Investigation Agency (FIA).[17] In situations where a warrant is obtainable but not without the 'apprehension of destruction, alteration or loss of data…devices or other articles', agents can still conduct searches and seizures without a warrant.[18] Section 35 goes on to further detail the powers of the authorised officer, including but not limited to accessing and inspecting information systems, obtaining and copying relevant data from these systems, requiring persons with decryption tools of an information system to grant access to encrypted information and require persons to give technical assistance in retrieving data and information.[19]

Information systems that generate this data, such as telecom companies and internet service providers (ISPs), are mandated under PECA to retain specified traffic data for at least one year.[20] The Monitoring and Reconciliation of Telephony Traffic Regulations Act, 2010 also 'obliges each local and international service provider to ensure the monitoring [and storage] of all data'.[21] With this requirement in place, the State can expand its network through dataveillance by having a readily accessible pool of data collected and retained by private service providers. It would be difficult for the State to have sufficient resources to establish an extensive surveillance network hence, its partnership with private companies allows it to access data that it otherwise would not be able to cultivate. In return, these companies and service providers are protected through a legal liability limitation per Section 38 of the PECA, a feature missing in the EU's General Data Protection Regulation

[15] Yasir Abbas 'Comparative Analysis: Digital Media Regulatory Landscape in Pakistan' (2022) Media Matters for Democracy <https://mediamatters.pk/wp-content/uploads/2022/10/Digital-Media-Regulatory-Landscape-in-Pakistan.pdf> accessed 29 December, 2022
[16] Shmyla Khan 'Year in Review: PECA' (*Digital Rights Foundation* n.d) <https://digitalrightsfoundation.pk/year-in-review-peca/> accessed 29 December 2022.
[17] Prevention of Electronic Crimes Act, 2016 ('PECA'), s 31(1).
[18] ibid s 33(2).
[19] ibid.
[20] ibid s 32(1).
[21] Dr. Akbar Nasir Khan, *Privacy & Surveillance Public Preferences in Pakistan* (1st edn, IRD 2021) 57.

(GDPR) which places complete liability for any breach of consumer data on data controllers and processors.[22]

Therefore, PECA provides legislative backing for the State to surveil and curtail dissent by having broad and invasive access to digital and electronic data. Its implementation is seldom concerned with the original legislative intent behind why the Act was promulgated; rather, it is now another tool of surveillance and control. For instance, in May 2017, 'a list of 200 social media activists was forwarded by the Interior Minister' to the National Response Centre for Cyber Crime for 'defaming the army.'[23] These actions implicate private citizens and criminalise them for exercising their right to free speech, with the potential to impact journalism.[24] It interferes with democratic processes as most of these activists were members of opposition parties, indicating that the Act is utilised as a tool for political victimisation.[25]

1.2.1 The Punjab Safe Cities Authority

With the current legislative framework and the State's partnership with private service provider companies discussed, another mode through which surveillance is carried out is through the widespread use of CCTV cameras and their collected footage, all of which operate under the mandate of the Punjab Safe City Authority (PCSA).

In Pakistan, the first Safe City Project was deployed in Islamabad in May 2015, and by October 2016, the Lahore Safe City Project was also operationalised.[26] Following these developments, the government launched

---

[22]Article 82 of the GDPR contains numerous provisions dealing with data controller and processor liability. Article 82(1) establishes the right of the data subject to claim compensation from data controllers/processors if they have suffered material or non-material damage as a result of an infringement of the GDPR. Article 82(2) holds that a controller involved in data processing will be responsible by the damage caused by processing that infringes the GDPR. Article 82(4) imposes joint liability for controllers and processors where both have been involved. While limited liability is a question in data protection, the GDPR makes its stance clear and attributes complete liability in order to uphold its high data protection standards.

[23] Khan (n 16).

[24] Furqan Mohammed 'PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill' (2016) 15 UCLA Journal of Islamic and Near Eastern Law 71 <https://escholarship.org/uc/item/14x2s9nr> accessed 29 December 2022.

[25] Khan (n 16).

[26] Akbar Nasir Khan, *Privacy & Surveillance Public Preferences in Pakistan* (1st edn, IRD 2021) 56.

seven more such projects in major city centres, which upon being implemented will potentially result in almost 40% of Punjab's population being surveyed through CCTV cameras.[27] The presence of CCTV cameras as a mode of public surveillance is particularly troubling, considering how it has allowed for an unprecedented level of intrusion in the lives of citizens in the public sphere.[28] While a variety of cogent justifications exist advocating for the use of CCTV cameras primarily in crime deterrence and aiding investigations, there is a unique risk presented by these cameras that host a vast pool of surveillance footage and facial-recognition tools which requires an enhanced mechanism for the protection of data gathered by them.[29] Under Article 5, the GDPR mandates that this footage is 'processed lawfully, fairly and in a transparent manner' and is not used for purposes beyond the scope of its objective.[30] Moreover, the data collector is mandated by the GDPR to maintain the security of CCTV cameras, and routinely delete footage.[31]

While the PSCA does try to protect privacy rights and provide data sharing and handling guidelines[32] through their Data and Privacy Protection Procedures (DP3),[33] these guidelines are inadequate due to the absence of national data protection regulations that can mandate how Safe City stores and uses data.[34]

Jannat Ali Kalyar, a lawyer and advocate who has previously worked as a Legal Officer in the Digital Rights Foundation and has been a Legal Executive in the Ministry of Information Technology and Telecom, Pakistan, states that during her years of practice, she has seen cases where PSCA officials have been involved in blackmailing private citizens through CCTV footage.

---

[27] ibid 56-7.
[28] IFSEC Insider, 'Role of CCTV Cameras: Public, Privacy and Protection' (IFSEC Insider, 1 Jan 2021) <https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/> accessed 20 November 2023.
[29] ibid.
[30] Muhammad Waqas Javed, Nazar Hussain, Muhammad Arbab Maitla 'CCTV Cameras Surveillance, Data Protection & Privacy Under International Human Rights Law' (2021) 3(2) Journal of Law and Social Studies 174, 181.
[31] ibid 182.
[32] Nasir Khan (n 21) 88.
[33] Nabeel Ahmed, 'The Promise and Peril of 'Safe City' Initiatives in Pakistan' (*Digital Rights Monitor*) <https://digitalrightsmonitor.pk/the-promise-and-peril-of-safe-city-initiatives-in-pakistan/> accessed 29 Dec 2022.
[34] ibid.

Officials capture videos of private citizens in compromising positions, trace their identity using car number plates and facial recognition technology in these cameras, and then extort the concerned individuals. While these specific actions may be committed by certain PSCA employees and not necessarily the State, it still highlights the ease with which CCTV data can be misused, especially where PSCA's project of setting up thousands of cameras across Punjab has inadvertently established a robust surveillance network. Even the State has certainly been involved in accessing footage from these cameras. Current IGP Islamabad, Dr Akbar Nasir Khan, writes that 'many senior officers in important organisations who were trying to enhance their control' have requested video data streaming from PSCA both through formal and informal means and upon refusal to disclose this data, he was placed under pressure and criticism for not indulging these 'mighty officers'. In one instance, he was even transferred from his position so that unauthorised access to data could be given to the establishment.[35] Ultimately, devising laws for regulating and protecting data is insufficient, as the PSCA lacks meaningful implementation of these rules and does not apply the DP3 in letter and spirit.[36]

These instances of State surveillance through PSCA CCTV cameras are described clandestinely, and there are hardly any publicly available resources that document the misuse of these cameras. This showcases that the State has created a sophisticated, tiered system of surveillance that is often well-concealed from the public eye, and there is a lack of coherent understanding of the scale of the State's surveillance machinery.

1.2.2 Surveillance and National Security

All States and their branches of government carry out surveillance to varying extents to protect State interests. It is natural for a State to be concerned with matters that they deem relevant to national security and their sovereignty, and surveillance is a tool through which they can track dissent and developments they perceive as threats. Ultimately, the issue arises when the ambit of national security and State interests is so broad that it creates an overreach in State

[35] Nasir Khan (n 21) 101.
[36] ibid.

powers; a 2013 UNSR report upheld that vague restrictions in the name of 'national security' could be used by the State as justifications to survey citizens and manipulated to target vulnerable groups.[37] That, alongside laws that legitimate State surveillance creates an environment where the fundamental rights of citizens are infringed upon, civil society members are under threat, and opposition can be politically victimised.

The State is concerned with preserving its authority, compelling it and its appointed agents to create a surveillance network upheld and regulated by law to bolster its legitimacy. Article 54(1) is profoundly important in the Pakistan Telecommunications Act as it reflects this concern. It creates an exception for national security, stating that '...in the interest of national security or the apprehension of any offence, the Federal Government may authorise any person or persons to intercept calls and messages or to trace calls through any telecommunication system'.[38] What the statute considers a State of 'national security' is unclear as the term remains undefined. Due to the broad and vague nature of the term with no limitations on its use, the State is empowered to carry out wiretapping across any telecommunication system for reasons they deem fit, which is another way to expand their surveillance network.

Wiretapping violates the fundamental human rights guaranteed under the Constitution of Pakistan. It is ultra vires to the right to privacy and dignity of citizens, enshrined in Article 14. The landmark *Benazir Bhutto* case dealt with the 'issue of tapping the telephones of judges, political leaders and military officials by the ruling government', and it was held in the judgment that 'tapping of phones and eavesdropping on citizens is a violation of the right to privacy guaranteed under Article 14 of the Constitution', and if tapping were to be allowed legally, it can be done when the country's security is under risk.[39] The Court upheld the dissolution of Bhutto's government. In their individual opinions, Justices Akhtar and Ilahi Khan ordered that since the existing Telegraph Act failed to regulate phone tapping, 'any communications

[37] Noor Ejaz Chaudhry, 'Big Brother: Mapping State Surveillance of Citizen Online and Offline' (*Digital Rights Monitor*) <https://digitalrightsmonitor.pk/pakistan-as-big-brother-mapping-state-surveillance-of-citizens-online-and-offline/> accessed 30 December 2022.
[38] Pakistan Telecommunication (Re-organization) Act, 1996, s 54(1) ('PTA').
[39] Srinivasan and Khandhadai (n 11) 32.

surveillance carried out by the government in the future must be done with the prior permission of the Supreme Court or by a Commission constituted by the Supreme Court which shall examine each case on its merits.'[40] Although this judgment has a progressive stance on the right to privacy and condemns surveillance overreach by the State, it cannot be read without keeping the country's political context in mind.

Advocate Kalyar shared her insight regarding the Benazir Bhutto case, which she stated was a progressive judgment 'on paper' but in actuality was likely politically motivated, keeping in mind the political turmoil in the 1990s that saw a constant tussle of power between the PML-N and PPP governments. What gives more evidence to the assumption that the judgment was not very concerned with curbing State surveillance is that it has not been followed up on nor been a part of mainstream discourses around privacy and surveillance. The safeguards outlined by the Justices have not been enforced; successive acts do not adopt those safeguards. In Advocate Kalyar's words, the Benazir Bhutto case can be considered 'irrelevant' to the discourse around digital rights and State surveillance today.

Ultimately, bounds to State surveillance must be established and enforced, and national security and State interests must be well-defined and well-articulated terms in order to strike a balance that allows for the State to be vigilant and protect national interests in a manner that doesn't infringe upon human rights and democracy.

2. STRIKING A BALANCE: THE RIGHT TO PRIVACY AND SURVEILLANCE

2.1 International Analysis

The protection of privacy is a significant consideration for any guiding international law frameworks, and hence, surveillance mechanisms established by countries should aim to be aligned with the standards set by international law. The International Covenant on Civil and Political Rights (ICCPR) does not explicitly define privacy as Article 17(1) mentions that

[40] ibid.

everyone is protected from unlawful interference with their 'privacy, family, home or correspondence'.[41] However, the Human Rights Council has issued recommendations that ensure that States comply with the principles of 'legality, necessity and proportionality' when interfering with citizens' privacy.[42] As such, legislation must specify the detailed circumstances in which privacy can be breached. Interference is only allowed if it is considered not to be arbitrary or unlawful. The Council defines these terms further and mentions that interference becomes arbitrary or unlawful in two circumstances: when the law does not sanction it, or when the interference or the law sanctioning it conflicts with the ICCPR. Hence, a breach of privacy becomes legitimate if it is in line with the law and the principles of the Covenant, necessary and proportionate to achieve a legitimate outcome, and the least intrusive option available. Such a framework treats privacy as the centre of all surveillance networks rather than as an expendable part of it.

The EU's General Data Protection Regulation (GDPR) is a model framework for protecting citizens' privacy[43] by focusing on 'lawfulness, fairness and transparency of processing; purpose limitations; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability'.[44] While not *ipso facto* binding on Pakistan as the country is not a signatory to it and nor an EU Member State, the regulations set a 'new threshold for international good practices' as it builds on existing OECD Privacy Principles and hence acts as an 'important reference point for global work in this area.'[45]

Under the GDPR, personal data directly or indirectly identifying an individual 'must not be collected, stored, or processed' without an appropriate legal

---

[41] American Civil Liberties Union, *Informational Privacy in the Digital Age* (ACLU, New York 2015) <https://www.aclu.org/documents/human-right-privacy-digital-age>

[42] Human Rights Council, 'Human Rights Council Holds Clustered Interactive Dialogue on the Right to Privacy and on Cultural Rights' (*UN Office of the High Commissioner of Human Rights*, 1 March 2019) <human-rights-council-holds-clustered-interactive-dialogue-right-privacy-and>

[43] Jannat Ali Kalyar, 'Protecting the Data A Comparative Analysis of Pakistan's Personal Data Protection Bill, 2020' (2021) *Media Matters for Democracy* <https://mediamatters.pk/wp-content/uploads/2021/02/Comparative-Analysis-of-Personal-Data-Protection-Bill-2020.pdf>

[44] Colin J. Bennet 'The European General Data Protection Regulation: An instrument for the globalization of privacy standards?' (2018) 23 Information Polity 240 <https://web.archive.org/web/20180720050914id_/https://content.iospress.com/download/information-polity/ip180002?id=information-polity%2Fip180002>

[45] Julia Clark, 'Practitioner's Guide: Data protection and privacy laws' (*The World Bank, Identification for Development* n.d) <https://id4d.worldbank.org/guide/data-protection-and-privacy-laws>.

basis.[46] Article 6 of the GDPR lists six bases upon which data controllers can lawfully process personal data. First, as per Article 6(1)(a), data can be lawfully processed with 'freely given, specific, informed and unambiguous' consent,[47] separately obtained for each processing action.[48] For special data categories, explicit consent needs to be given in writing.[49] Secondly, under Article 6(1)(b), data can be processed when necessary for a contract's performance. To this end, it must be objectively necessary in order to execute the performance of a contract,[50] or where a formal contract does not exist but the subject intends for it to and they request the controller to process the data before entering into the contract.[51] Thirdly, processing is allowed when it is necessary for compliance with a legal obligation the controller is subject to.[52] 'Legal obligations' can mean common law or statutory principles.[53] For this, personal data must be strictly required, and controllers should be able to specifically point out what legal obligation makes it necessary for them to obtain personal data.

Next, personal data can be processed when it is necessary to protect the interests of the data subject or any other natural person.[54] For this, the controller should prove that they are not able to reasonably protect the subject's vital interests in some other way. But this can be bypassed in cases of emergencies, such as if a health risk is involved. Fifth, personal data can be processed when it is necessary to carry out a task in the public interest or official duty.[55] To this end, the controller must point to a benefit to society rather than a benefit to a specific interest or individual.[56] Lastly, personal data

---

[46] Elena Gil Gonzalez and Paul de Hart, 'Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles' (*ERA Forum*, February 2019) <https://link.springer.com/article/10.1007/s12027-018-0546-z#citeas>.
[47] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 ('GDPR').
[48] Gonzalez and de Hart (n 46).
[49] GDPR, art 9.
[50] Privacy Research Team, 'Article 6 of the GDPR: Explained' (*Securiti*, 24 June 2022) <https://securiti.ai/blog/article-6-gdpr/>.
[51] Ibid.
[52] GDPR, art 6(1)(c).
[53] Privacy Research Team (n 50).
[54] GDPR, art 6(1)(d).
[55] GDPR, art 6(1)(e).
[56] Privacy Research Team (n 50).

may be processed necessary for legitimate interests pursued by the controller or a third party, except when the interests conflict with the data subject's fundamental rights, especially when they are a child.[57] Here, 'interest' qualifies as the 'intention' the controller wishes to fulfil with the information, and legitimacy comes from it respecting not just data protection laws but all laws. To this end, it must be 'real, present, and articulated'.[58]

The controller must inform data subjects about the legitimate interest[59] with a necessity and balancing test in place to justify the legitimacy of the interest. The balancing test involves weighing the requestor's interest on one side and the data subject's on the other.[60] Necessity denotes that the data processing be directly linked to achieving the interest and that no other less intrusive way is available; however, if the other way is deemed to require a disproportionate effort, then the process can still be considered necessary. These six exceptions provide comprehensive protection for citizens' privacy rights in the face of data collectors working for different organisations.

A critique can be made that the GDPR does not apply to mass-scale government surveillance; State agencies can access personal data without consent if a concern relates to 'national security', 'defence', or 'public security'.[61] However, the EU's Court of Justice has established that these terms do not provide carte blanche for countries to obtain any kind of data however they please.[62] They are still subjected to national and international human rights laws and national regulations that do not go against EU regulations.[63] Each EU member State is given the liberty to balance national security with data protection provided any limitation on privacy rights is 'necessary and proportionate'.[64] A core issue addressed by the court was how

[57] GDPR, art 6(1)(f).
[58] Gonzalez and de Hart (n 46).
[59] ibid.
[60] ibid.
[61] Human Rights Watch, 'The EU General Data Protection Regulation' (*Human Rights Watch*, 6 June 2018) <https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation>.
[62] ibid.
[63] ibid.
[64] Kerry CF and others, 'The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security' (*Brookings*, 9 March 2022) <https://www.brookings.edu/articles/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/>.

national security agencies can balance security interest with adequate data protection consistent with the GDPR. To this end, it was examining the US government's access to EU citizen's personal data for national security purposes, alongside their right to judicial review or redressal in the US. It held that transfer of data to a third country, even if for national security reasons, is still governed by the GDPR, therefore, whenever an EU citizen's data is transferred abroad, they must be afforded the same protections, rights, and liabilities they are guaranteed in Europe. It further concluded that US national security requirements infringed on the fundamental rights of individuals whose data was transferred there. The principle of proportionately was not satisfied either as US surveillance was not only conducted when 'strictly necessary'.[65]

When such a framework is applied to States, their mechanisms for protecting privacy rights are enhanced. In a study conducted by Comparitech, it was found that countries in the European Union improved data safeguards provided by the government and adopted more equitable regulations, mainly due to the implementation of the GDPR.[66]

The GDPR has been implemented successfully outside the EU as well. In Norway, companies have begun to invest more in compliance efforts, and there is a more receptive attitude towards data protection.[67] Due to stricter regulations, the country's DPA imposes fines on public sector entities who process data without following guidelines, therefore not adhering to the condition of only doing so on a legal basis. For example, a private sector organisation was fined for sending data obtained from illegal camera surveillance to China without a proper 'data processing agreement'.[68] Fines were also issued to companies in the United States; for example, the dating

[65] ibid.
[66] Paul Bischoff, 'Data privacy laws & government surveillance by country: Which countries best protect their citizens?' (*Comparitech*, 15 October 2019) <https://www.comparitech.com/blog/vpn-privacy/surveillance-states/>.
[67] Pat Brans, 'Four years into GDPR, Norway hopes for safer data transfer to US' (*Computer Weekly*, 31 August 2022) <https://www.computerweekly.com/news/252524408/Four-years-into-GDPR-Norway-hopes-for-safer-data-transfer-to-US>
[68] ibid

network Grindr was fined €6.5m by the DPA for sharing user data with unknown third parties without user consent.[69]

3. THE RIGHT TO PRIVACY WITHIN PAKISTAN'S SURVEILLANCE FRAMEWORK

As mentioned earlier, Pakistan's surveillance framework consists of numerous statutes, mainly the PECA, and projects under the mandate of the PSCA. All these statutes, projects and actions present different modes by which the State machinery carries out surveillance and how this surveillance is protected under the law. After analysing how an appropriate balance can be struck between the right to privacy and State surveillance through international examples, such as GDPR, we can begin to dive into the discussion of how the Constitutional right to privacy is not adequately protected within Pakistan's surveillance framework, with a focus on specific provisions of the PECA, the Pakistan Telecommunications Act, and Fair Trial Act that infringe upon the right to privacy.

3.1 The Pakistan Electronic Crimes Act, 2016

Various provisions of the PECA disregard privacy rights, and this can be seen through a mix of unfettered powers given to authorised agents, a lack of protection protocols, and weak implementation of clauses that intend to protect privacy. Section 32 allows service providers to retain specified traffic data for at least one year or any other time that the Pakistan Telecommunication Authority (PTA) deems fit.[70] Furthermore, section 32(2) mentions that service providers must follow retention guidelines given under sections 5 and 6 of the Electronic Transactions Ordinance, 2002 (ETO). [71]

The problem here is two-fold. First, the section sanctions retention without mentioning any data protection protocols that would dictate how this information is kept secured. This means the data retained for a year is susceptible to breaches. As it is sensitive data, it represents an individual's

[69] ibid
[70] PECA, s 32.
[71] ibid s 32(2).

digital footprint that can be used to ascertain their location, communicate with others, etc.[72] The value of this data was affirmed by the Supreme Court of the Philippines, which struck down the data retention requirement in their cybercrime law as it held that the requirement infringed on the privacy of the users and the data was too telling to be kept without proper safety protocols.[73]

Secondly, there is a lack of clarity concerning when this data can be extracted. The section mentions that it can be retained whenever required; however, there is no expansion as to what warrants keeping this data. Section 32(2) references the ETO, but the relevant sections only provide details on what constitutes legitimate data. For example, section 6 mentions that the requirement that certain data be retained in electronic form is fulfilled if its contents remain accessible for 'subsequent reference' if its content and form can accurately represent its original form, and if the data can enable the identification of its origin and destination, etc.[74] A plain reading shows that this only refers to the form in which the data should be, not the criteria under which it can be taken. Furthermore, a purview of case law shows us that the ETO 2002 sections mentioned serve evidentiary rather than substantive purposes.[75] In this way, we are left with no understanding of what situations or circumstances allow one's right to privacy to be breached by keeping their data for a year, especially with no protection protocols in place.

Section 39 of the PECA allows for the real-time collection and recording of information for seven days that can be extended. For this, the court requires information from an authorised officer who has reasonable grounds to believe that any data is required for a specific criminal investigation.[76] While the section extensively mentions the substantive and procedural grounds needed for an application to collect real-time data and the importance of protecting the privacy of other users, customers, and third parties, it leaves

[72] Bolo Bhi, 'Major Contentions: PECA' (*Bolo Bhi*, 2016) <http://bolobhi.org/wp-content/uploads/2016/10/Major-contentions-PECA-2016.pdf>.
[73] *Disini v The Secretary of Justice* [2014] 727 Phil. 28.
[74] Electronic Transactions Ordinance, 2002, s 6.
[75] *Alamgir Khalid Chughtai v The State* (PLD 2009 Lah 254).
[76] PECA, s 39(1).

out the limits of this data collection on the data subject.[77] In this way, local law enforcement can use invasive measures to monitor citizens. Due to PECA not mentioning the scope of this collection, the section enables various unchecked modes of surveillance that disregard one's right to privacy.

Furthermore, section 42 of the PECA mentions international cooperation and lists down how the government would cooperate with a foreign government if they made a data request.[78] While the section establishes reasons for the government refusing a request, there is no mention of the decision-making process for accepting requests. This lack of transparency leaves citizens vulnerable to surveillance from foreign governments.[79]

3.2 The Pakistan Telecommunication (Re-organisation) Act, 1996

Section 54 of the Act allows the Federal Government to authorize any person or person to intercept calls and messages or to trace calls in the interest of national security.[80] Interestingly enough, the Act does not define national security. However, section 54(2) mentions that the Federal Government will have 'preference and priority' over telecommunication systems in the event of war or any other hostilities in Pakistan.[81] With this, the State obtains unbridled legal powers to obtain any data from telecommunication companies under the guise of national security. Due to this, there is no check-and-balance over what kind of information the State machinery is extracting, and there is no expansion of what constitutes national security within statutes. The concern over government actions under the guise of national security have been raised even in the Apex Court, with a five-member bench affirming that the government cannot commit constitutional breaches and escape scrutiny under the claim of national security, unless these concerns are evidenced and well-defined.[82] As a result, we see the ambit of national security being misused to infringe on people's right to privacy and prosecute them for

[77] Media Matters for Democracy 'White Paper on Reforms for the Prevention of Electronic Crimes Act (PECA) 2016' (Media Matters for Democracy, May 2020) <https://www.cpdi-pakistan.org/wp-content/uploads/2021/01/WPPecaReforms-refined.pdf>
[78] PECA, s 42(1).
[79] Media Matters for Democracy (n 77).
[80] PTA, s 54.
[81] ibid s 54(2).
[82] *Pakistan Peoples Party Parliamentarians v Federation of Pakistan* (PLD 2022 SC 574).

crimes such as blasphemy and sedition, that may arguably be of concern for State interests but absolutely do not fall under the ambit of national security. Hence, surveillance can be carried out that infringes upon the privacy of citizens and policies and punishes them on the basis of vague terminology that encompasses a vastly wide variety of matters empowering the State to take any action it deems fit.

3.3 The Investigation for Fair Trial Act, 2013

This Act intends to provide a framework for the collection of evidence through evolving techniques that regulate the powers of law enforcement and intelligence agencies. Ultimately, it sets up ways that user data can be accessed and circumstances in which the right to privacy can be breached in the interest of gathering evidence and providing for a fair and speedy trial. Section 5 allows any official or applicant to prepare a report with supporting material looking to obtain a warrant for surveillance on someone that they feel is likely or going to commit a scheduled offence.[83] Subsequent sections lay out the procedure for doing so and mention that the officer must go to the Minister through the Head of the Department before obtaining the warrant. Section 9, however, mentions that an officer can obtain a warrant for surveillance from a judge in their chambers.[84] The conditions for this warrant being granted are listed in section 10. The entire Act is meant to bypass a citizen's right to privacy and enable surveillance without considering the interests of the data subject. While some sections do lay out a thorough procedure where the report goes through multiple checks, section 9 sanctions secret warrants to be given in the judge's chamber, bypassing approval from department heads or ministers.[85] This Act is another example of how a breach of the right to privacy is justified under the guise of national security without taking into consideration the plethora of boundaries and procedures that other frameworks, such as the GDPR, take when allowing for data processing.

[83] Investigation for Fair Trial Act, 2013 ('FTA'), s 5.
[84] ibid s 9.
[85] ibid.

4. THE WAY FORWARD

When compared with the kind of considerations that the international human rights privacy framework incorporates, it becomes clear that Pakistan's surveillance framework fails to uphold the constitutional right to privacy.

The three legislative documents analysed for this paper exhibited the State's prioritisation of self-interest over the rights and freedoms afforded to protect the privacy of its citizens. When compared with the GDPR, the FTA 2013 and PTA 1996 do not address the data subject's consent. PECA 2016 mentions this in section 41, however, it is seldom implemented.[86]

Furthermore, unlike the GDPR, there are no tests available to determine whether surveillance is necessary for a situation and if the rights and interests of the data subjects have been balanced against those of the State. The crucial test of seeing whether there are alternative, less intrusive ways of obtaining data is also missing within all the legislative frameworks we analyzed. As such, we see that vital considerations to protecting privacy rights while maintaining the need for State security are absent within the frameworks in Pakistan, and as a result, we see the right to privacy shrinking within society.

4.1 Data Protection Bill

In order to reform the current framework, Pakistan can look towards a comprehensive data protection bill. Currently, there are numerous sections in multiple acts that regulate data protection indirectly. For example, section 36 of the ETO criminalizes accessing or trying to access unauthorised data; the Ordinance also mentions the establishment of a body that can make regulations for the protection of its users.[87] Similarly, section 17 of the Freedom of Information Ordinance exempts certain forms of information from disclosure if it would lead to the breach of an individual's privacy other than the requester. Moreover, case law gives us valuable examples of the

[86] Hija Kamran 'Privacy-in-Law: How safe is your data?' (*Digital Rights Monitor,* 27 September 2019) <https://digitalrightsmonitor.pk/privacy-in-law/>.
[87] Electronic Transaction Ordinance, 2002, s 43(2)(e).

increasing recognition of privacy.[88] Notably, in *M.D. Tahir, Advocate v The Director, State Bank of Pakistan, Lahore and 3 others,* the court held that presenting the private information of bank holders to tax authorities, with no allegation of wrongdoing, was illegal, as the individuals had trusted the bank under a fiduciary relationship.[89] Even though data protection is recognised through various avenues in the law, there is a need for a codified document that can act as the authority on this matter.

Since 2018, legislators have been attempting to introduce a law that directly addresses data protection through the Personal Data Protection Bill (PDPB). The fifth iteration of the Bill,[90] introduced in 2023, takes extensively from the GDPR and presents a comprehensive set of provisions that touch on various issues. The PDPB is arranged in sections specifically touching upon the obligations of data controllers and processors, the rights of data subjects, processing of children's data, requirements for processing sensitive and critical personal data, transferring personal data outside Pakistan, exceptions, and penalties. While it has rectified mistakes from previous editions, the 2023 draft has alarming provisions allowing governments to survey citizens without respect for their privacy, particularly through supervisory authorities, data localisation, ambiguous data and security definitions, and irregular processes surrounding consent.

4.2 Supervisory Authorities (National Commission for Personal Data Protection)

While the PDPB has been modelled on the GDPR since its inception, certain provisions stand out as going against international data protection standards. Take the example of Supervisory Authorities (SA). Recital 117 sets out an integral part of the GDPR: States should establish Supervisory Authorities, and 'exercise their powers with complete independence…'.[91] This is to ensure that governments do not intervene in data protection infrastructures to serve

[88] Freedom of Information Ordinance, 2002, s 17.
[89] *M.D. Tahir, Advocate v The Director, State Bank of Pakistan, Lahore and 3 others* (2004 CLC 1680)
[90] Personal Data Protection Bill, 2023 <https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf> ('PDPB').
[91] GDPR, recital 117.

their own benefits. Its independence is necessary as it is responsible for hearing complaints from data subjects regarding data protection and possesses a series of authoritative, advisory, investigative and corrective powers.

To this end, SAs are meant to be 'independent public authorities' responsible for protecting the fundamental rights of data subjects.[92] In exercising this role, they should 'remain free from external influence' and not 'take instructions from anybody'.[93] The government has to ensure that the SA chooses its staff, which is 'subject to the exclusive direction' of its members. Members of the SA should be appointed by the Parliament, Government, Head of State, or any independent body entrusted with the appointment, but by 'means of a transparent procedure'.[94]

Chapter 8 of the PDPB 2023 fulfils the SA requirement with the National Commission for Personal Data Protection (NCPDP). Section 35(2) holds that the Commission 'shall be an autonomous body under the administrative control of the Federal Government'.[95] While this is a practice followed by EU Member States as well, problems arise when we come to the workings and composition of the Commission. As mentioned earlier, the GDPR makes it imperative that the selection process for the Commission is transparent. However, the PDPB 2023 mentions no selection process, simply stating that the Chairman and four full-time Members will be appointed on the Federal Government's recommendation.[96] The vague wording for selection goes against international principles to uphold a transparent selection criteria. In comparison, the United Kingdom publishes a report on the appointment of the Information Commissioner, detailing how the selection was made, the criteria followed, the number of applicants, and reasons for selecting the preferred candidate.[97]

---

[92] ibid art 52.
[93] ibid.
[94] ibid.
[95] PDPB, s 35(2).
[96] ibid s 36(1).
[97] House of Commons Culture, Media and Sport Committee, *Appointment of the Information Commissioner* (House of Commons Second Report of Session 2015-16, 2016).

Furthermore, sections 36(4) and 38(3) mention that all members and staff of the Commission will be considered public servants, meaning that they will be subject to all the conditions imposed on public servants. The implications of this are broad, as public servants are often at the government's mercy and must adhere to directives and policies. By making members and staff of the Commission public servants, the government takes away the impartiality required by international data protection standards. The independence of the Commission is further challenged in section 43 which empowers the Federal Government to 'issue policy directives' to the Commission on matters regarding data protection 'as and when required'.[98] The Federal Government 'mandates' the Commission to follow these directives. Under a government that prioritises national security over data protection, such vague clauses can lead to selfish misuse, harming citizens' right to privacy, particularly because section 44(3) allows the government to request any information from the Commission, the nature of which has no restriction. The lack of independence can also hamper international collaboration as section 47 holds that the Commission can only cooperate with foreign authorities and international organisations on matters of data protection, privacy, and theft, subject to the approval of the Federal Government.

4.3 Critical and Sensitive Personal Data

The PDPB 2023 creates two categories of data: 'critical personal data' and 'sensitive personal data'. The former is unclearly defined as personal data retained by the public service provider (any entity that has and deals with personal data while working with the government) and classified as such by the Commission or relates to international obligations. The latter takes from the GDPR and is defined as personal data referring to financial information, health data, CNIC or passport, biometric data, genetic data, religious beliefs, criminal records, political affiliations, caste or tribe, and ethnicity.

Apart from keeping the definition of critical personal data particularly vague, the State limits its processing to servers located within Pakistan.[99] This data localisation requirement allows governments to exhibit control over this data

[98] PDPB, s 43.
[99] ibid s 31(2).

and the service providers controlling it.[100] Critical personal data is anything that the Commission identifies as such. Since the Commission is closely tied to the government and can be mandated to reflect its interests, the government can surveil citizens by declaring data as critical personal and requiring that it remain in the country. Then, using the Commission's access it can obtain citizen data. This complex surveillance mechanism goes against both the right to privacy enshrined in the Constitution and upheld by various judicial opinions and international obligations found in the GDPR and ICCPR. Talking to advocate, data expert, and former visiting faculty at LUMS, Hassan Niazi, we learnt that Pakistan's intention with data localisation has historically been purely for national security reasons, making the localisation requirement much more alarming.

Surveillance of sensitive personal data is more explicit as section 32(2) empowers the Commission to conceive a mechanism to share the data with the government for public order or national security. Concerns regarding the definition of national security have been brought up in this paper and by other academics throughout previous iterations of the PDPB, and the 2023 edition fails to rectify this. This provision allows the government to obtain sensitive personal data at will and without facing accountability because national security is a term defined to serve whatever interest it is pursuing.

4.4 Withdrawal of Consent

Article 7 of the GDPR mentions that the withdrawal of consent shall be as easy as giving consent, often done through one-step and accessible systems. The spirit behind this is to ensure there are no hurdles in withdrawal for a data subject. Although the PDPB 2023 has significantly improved in incorporating international obligations surrounding consent, this principle is missing. Section 6(1) says that a data controller must obtain an individual's consent but does not mention how it should be done and only refers to the fact that it must be 'free, specific, informed, and unambiguous'.[101] In contrast, section 23(1) requires a data subject to give a written notice if they want to withdraw consent.

[100] Mian Sami ud-Din, 'State on Surveillance' *The News* (9 August 2023)
[101] PDPB, s 6(1).

The vague wording leaves the process of procuring consent unclear; if the procurement process is not specified, how will an adequate standard of consent be guaranteed? This leaves citizens' right to privacy prone to surveillance as a manipulation of the process could lead to their data being used without approval. Moreover, the inconsistency between the obtainment and withdrawal processes goes against the requirements set by the GDPR and limits the accessibility of withdrawal. The requirement of a written notice excludes those who are illiterate making it more difficult to withdraw consent than obtain it.

5. CONCLUSION AND RECOMMENDATIONS

Pakistan's surveillance machinery exists so that the State can maintain its overreaching authority through dataveillance and wield the information gained from it to dispense discipline and control. Within this monopoly of power, legitimated by a legislative framework, it is clear that the right to privacy for citizens remains unprotected. All these surveillance actions are justified by the State under the guise of national security and protecting State interests. There are no checks and balances that can regulate State overreach and protect the fundamental human rights of citizens. Moreover, more cognisable effort is required to bring Pakistan's laws in compliance with international human rights standards such as those set out in the ICCPR or the recommendations made by the Human Rights Council that act as guiding principles for States when intruding on citizens' privacy.

On a judicial level, it is integral to establish the necessity and balancing tests with PDPB. With the GDPR, this has become a practice, hence its absence in the Pakistani bill can cause discrepancies. A legal framework influenced by jurisdictions, such as India, can be followed. In *Justice K.S.Puttaswamy (Retd) v Union Of India*, the importance of the right to privacy was acknowledged and a three-fold test was laid down for its restrictions.[102] The test involved checking into the legality of the restriction, checking the need (usually defined

[102] *Justice K.S.Puttaswamy (Retd) v Union Of India* [2017] AIR SC 4161

by the State in their aims), and checking proportionately.[103] Justice Kaul added a fourth dimension: 'procedural safeguards against abuse of interference with rights'.[104]

On another front, removing these laws of State interests requires complicated amendments only possible in a regime concerned about data protection, and even then the process is arduous, dependent on parliamentarians, and can take considerable time to bear fruit. Instead, it is more useful to focus on bridging the gap between the data protection bill and international obligations.

The glaring issue of an independent commission needs to be addressed. According to Advocate Niazi, transparency is an essential ingredient to an equitable data protection framework.[105] He mentions that activists have routinely submitted RTI applications[106] to bodies such as the PTA, but have not gotten any responses due to the lack of an accountability framework through which citizens can exercise agency over these bodies. Such legislative errors cannot be repeated with the new data protection framework.

Advocate Niazi holds that the appointment and removal of a body's members is a crucial consideration when determining its independence.[107] Hence, the NCPDP must ensure these two aspects are not left vague. Legislators can follow in the UK's footsteps and include rules for selecting members and setting up Parliamentary Standing Committees that can prepare reports on the selection criteria and process. In fact, it can look towards the Competition Commission of Pakistan (CCP) as inspiration, which serves a similar regulatory purpose to the NCPDP. The CCP was established under the Competition Ordinance, 2010. It exhibits transparency by detailing the standards to which its members are held and lists down situations under

---

[103] Nath K, 'Analysis of Right to Privacy in Modern Era' (*Finology Blog - Latest Updates & News on Current Affairs and Laws in India,* 2020) <https://blog.finology.in/constitutional-developments/analysis-of-right-to-privacy-india?fb_comment_id=3501071956617521_3525643984160318>

[104] Kalyar (n 43).

[105] Interview with Hassan Niazi, Previously Visiting Faculty, Faculty of Law, LUMS (Lahore, Pakistan, 25 November 2023).

[106] Right to information applications under Article 19A of the Constitution.

[107] Interview with Hassan Niazi (n 105).

which someone cannot be appointed or continue as a member; section 14(6) mentions reasons such as being absent from three consecutive commission meetings without taking prior leave or failing to disclose any conflict of interest. The PDPB lacks such standards for NCPDP members and incorporating them could be a useful step towards greater transparency, accountability, and independence.

Furthermore, members and staff should not be considered public servants to ensure impartiality. Once again, inspiration can be gathered from the CCP. Section 14(4) of the Competition Ordinance, 2010, holds that only two members of the commission can be employees of the Federal Government, effectively removing the direct involvement of government personnel within the commission. Section 35(4) mentions that the NCPDP is a statutory corporate body. Employees of statutory corporate bodies, such as the National Bank of Pakistan (NBP) and CCP, are not government or public servants. This was confirmed by the Supreme Court of Pakistan in 2019 after Justice Mansoor Ali Shah ordered that NBP employees remove their occupation as 'Government Employees' from their passports.[108] Hence, members and staff of the Commission do not have to be public servants which can help secure their impartiality.

Sections that allow the government to obtain any information from the Commission should be modified. The European Model sets up SAs for every Member State that comprise the European Data Protection Board. This allows them to make decisions and oversee consistent compliance with the GDPR democratically. Pakistan could mandate independent provincial commissions that together form a similarly independent national commission. This would allow collective deliberation and foresight over government requests and let the independent national commission act as a watchdog to ensure that data is consistently being protected across the country. All government directives and approvals can be filtered through the National Commission to see if they meet data protection regulations.

[108] *Muhammad Naeem v Federation of Pakistan* (2019 CP 4294).

However, as pointed out by Advocate Niazi, such a recommendation is contingent upon whether data protection is a federal or provincial subject.[109]

Moreover, the PDPB should refrain from promoting data localisation policies that permit the government to store important information. To effectively enact them, the country requires the expansive digital infrastructure that it currently lacks. However, it maintains data localisation for national security reasons, prioritising them over 'economic, trade, and human rights interests.[110] Data protection interests should be at the forefront of an internationally compliant data protection bill, which does not have room for data localisation that hinders the rights of data subjects.

To avoid vagueness and further room for surveillance, the bill should clearly define any data categories created or 'national/public interest'. 'Critical personal data' should be defined, either in the bill or through the rules of the Commission, and not left to an arbitrary choice of the independent supervisory authority. Alternatively, the criteria for declaring personal data as 'critical' can be transparently drafted and published in the bill or in the rules. In the same spirit, the process for obtaining and withdrawing consent should be unified to guarantee an equitable procedure with no entry barriers and compliance with international obligations.

Maria Khan, a data privacy legal manager at Securiti, suggests that for substantive modifications, the Ministry of Information Technology and Telecom must consider all perspectives and keep the spirit of international frameworks, such as the GDPR, in mind.[111] But, while borrowing its language, it should be careful not to overpromise, and ground legislation within Pakistani realities. As far as procedural modifications are concerned, she believes that they can be fixed easily if the ministry releases rules and regulations alongside the final data protection act. According to her,

---

[109] Interview with Hassan Niazi (n 105).
[110] Nigel Cory, Luke Dascoli and Ian Clay, 'The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam' (*Information Technology and Innovation Foundation,* 12 December 2022) https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/.
[111] Interview with Maria Khan, Data Privacy Legal Manager, Securiti (Lahore, Pakistan, 28 November 2023).

publishing drafts of the regulations, alongside the proposed bill, can help the ministry make better decisions and gain insight from a plethora of stakeholders, further taking a step towards transparency and inclusivity.

While Pakistan's surveillance network is complex, it suffers terribly from misguided priorities. The evolving data landscape requires more clarity regarding the rights of data subjects and the situations in which these rights can be infringed. It is only natural that a surveillance regime focused on national security and data collection protects citizen rights through a data protection bill. Pakistan has shown considerable promise towards the establishment of a comprehensive data protection infrastructure, however, there is a need to localise the law to fit the country's context. This includes making sure data systems are not so complex that they cannot be implemented, or so vague that they apply to all situations. Legislators should look towards the spirit of international data protection legislation, rather than copy its content, and strike a balance aiming to develop an equitable relationship between State interests and citizen rights.