
State Surveillance without Safeguards: Constitutional Limits on Digital Monitoring in Pakistan

Muhammad Usman Elif¹

¹ Advocate, B.A, LL.B, PGDCLP (PU), Email: usmaneliff@gmail.com

DOI: <https://doi.org/10.70670/sra.v4i1.2559>

Abstract

Despite being one of the biggest digital-governance infrastructures in South Asia, ranging from NADRA's biometric database to Safe City facial-recognition networks to PECA-enabled cybercrime investigation, the data these systems generate is not governed by any single law that regulates its collection, retention, sharing or judicial oversight. This article argues that the right to informational privacy is already broadly defined under Article 14 of the Constitution, and in combination with the rights provided by Articles 4, 9, 25 and 199, offers a good basis for requiring courts to adopt a proportionality test to information security practices. The article, based on the doctrinal analysis of the constitutional and statutory law of Pakistan, relies on comparative analysis of India, the United Kingdom, and the United States to recommend a proportionality and oversight framework for Pakistan and concrete legislative reforms in order to close the gap in the Pakistani surveillance accountability.

Keywords: Informational privacy; digital surveillance; proportionality; Safe City; Data Privacy; Right to Privacy; Fundamental Rights

Introduction

The digital-governance infrastructure in Pakistan has been one of the largest in South Asia over the past 10 years, but there is no commensurate constitutional framework to check its activities. Safe City projects include the integration of facial recognition analytics with CCTV networks in Islamabad, Lahore, Peshawar and Karachi, while NADRA has biometric and demographic data on almost the entire adult population and SIM registration and biometric verification and links all mobile connections to an identifiable identity. The Federal Investigation Agency (FIA) routinely extracts information from seized phones and social media accounts during cybercrime investigations as per Prevention of Electronic Crimes Act 2016 (PECA). All of these systems have been implemented to limit terror, to prevent crime, or to make things easier for administrators. Pakistan lacks a complete and uniform cross-sectoral system of data-protection and have no statute, a requirement for judicial warrants, an independent oversight body or an enforceable citizens' right of access and erasure of the data collected.

This gap isn't due to lack of constitutional text. According to Article 14 of the Constitution of the Islamic Republic of Pakistan 1973, the dignity of man and, subject to law, the privacy of the home, is inviolable, and the Supreme Court in a number of cases has interpreted this guarantee in a wide

fashion. In *Benazir Bhutto v President of Pakistan*, where the court declared that the tapping of telephones without statutory authority is reprehensible, immoral, illegal and unconstitutional.¹ The rights to life, liberty and equality (articles 9 and 25) have also been given a broader interpretation than their exact wording. Article 9 guarantees the right to life and liberty "save in accordance with law" and in the landmark environmental case of *Shehla Zia v WAPDA*, the Supreme Court held that the right to life under Article 9 is not just a bare biological guarantee rather the right to a dignified life free from unlawful interference by the state or third parties, a proposition that was incorporated into the current case to include surveillance harms.² However, all this jurisprudence that has arisen in Pakistan during the past four decades, virtually exclusively around telephone interception and physical search, has left the judicial largely silent to the tougher issues raised by biometric databases, algorithmic facial recognition, bulk metadata retention, and cross-agency data sharing all of which are now define day-to-day policing in the major cities of Pakistan.

Pakistan has a wide range of surveillance powers without having a clear constitutional framework for the collection, storage, sharing, judicial oversight and independent review of that power. There are some research questions and their answers had been given in this paper. Does informational privacy sufficiently safeguarded by the Pakistani Constitution? Do current powers of surveillance have any form of judicial oversight or do they only rely on internal executive authorisation? What changes are needed to balance legitimate national security and law enforcement goals with the constitutional liberty?

This article argues after deep analysis of Article 14, read in its context with Articles 4, 9, 25 and 199 of the Constitution of Pakistan 1973, that the right to informational privacy is already sufficiently broad to demand the judicial application of the proportionality framework to the intrusive nature of these forms of surveillance. Despite that, the right is not sufficiently enforced because Pakistani law does not provide the procedural protections currently afforded in other comparable common-law jurisdictions. The article then proceeds doctrinally, by examining the text of the Constitution and the decisions of the Superior Courts, bolstered by some comparative analysis of India, the United Kingdom and the United States, all of which have matured judicial or statutory answers to a problem that Pakistan has yet to solve: how to empower and oversee the government's access to digital records.

1. The Evolution of Privacy Rights: From Classical to Informational Privacy

The notion of privacy as a legal concept was originally a spatial guarantee. The first common-law expression of the rights of the home and the letter is the expression that a man's house is his castle, which was first articulated by Blackstone. This classical notion was inherited by Pakistani law, and the words of Article 14 itself refer to the privacy of home. While cases like *Manzoor Ahmad v The State* referred to the eavesdropping and covert photography of inside a house as the classical violation of privacy.³ The twentieth century redefined privacy in terms of autonomy instead of territory. Alan Westin's definition of privacy, which was influential, shifted from place to

¹ *Mohtarma Benazir Bhutto and Others v President of Pakistan* [PLD 1998 SC 388].

² *Ms Shehla Zia v WAPDA* PLD 1994 SC 693.

³ *Manzoor Ahmad v The State* [1990 MLD 1488 LHC].

information, saying that privacy was the right of individuals to decide when, how, and to whom information about them can be passed on.⁴ In turn, Daniel Solove broke this down into a taxonomy of specific harms, deeming privacy to be a bundle of problems that a legal system must solve apart.⁵ Another refinement was Helen Nissenbaum's contextual integrity theory, which states that information shared in one context (a hospital, a mosque, a courtroom) carries with it norms that are violated if the same information is taken, combined, or repurposed in a different context, even if there is no actual trespass.⁶ This is the conceptual shift imposed upon Pakistani constitution that digital surveillance demands. A citizen whose CNIC, fingerprints, phone location and facial geometry is spread across the NADRA's, the FIA's and the Safe City's databases has never been in "the home" in a traditional sense, but when all that data comes together, it creates the loss of autonomy, dignity and control that Westin, Solove and Nissenbaum speak of. Thus, privacy in its modern, informational sense is not an extension of the language of Article 14 in any sense; it is the same value of dignity and control over one's own life in an alternative technological medium. That's a doctrinal question for Pakistani courts; has Article 14 caught up with that change, or has it remained stuck in the home made walls where it was drafted?

2. Constitutional Protection of Privacy in Pakistan

Article 14(1) states that the dignity of man and the privacy of home, subject to law shall be inviolable. Textually connected to the home, a literal reading has never been accepted by the Supreme Court. The case of *Mohtarma Benazir Bhutto v President of Pakistan* involved a seven-member Bench which had to determine the constitutional validity of the intelligence agencies' use of telephone tapping without any legislative authorization.⁷ In the case of the Court, the Court held such surveillance to be unconstitutional based on the reasoning of Justice Saleem Akhtar in his concurring opinion, which relied on the precedent set by the *Katz v the United States* case that the constitution protects the "privacy of home" and that a person's privacy is not unprotected once out of the home.⁸ In the absence of any legislation the Court ordered that any such surveillance must first be approved by a court or a court-established committee. This was already suggested by the Lahore High Court in *Manzoor Ahmad v The State*, which had ruled that eavesdropping, hidden taping and snapping pictures inside a house is an invasion of privacy both under Article 14 and the Islamic law.⁹ In *M D Tahir Advocate v. Director, State Bank of Pakistan* the Supreme Court further held that the dignity-based interpretation of Article 14 had been strengthened since the telephone conversation was of a private and intimate nature and it was constitutionally protected from disclosure, even if the parties were physically located in a different place.¹⁰ This reasoning has since been expanded into other areas, in *Ghulam Hussain v Additional Sessions Judge, Dera Allah*

⁴ Alan Westin, *Privacy and Freedom* (Atheneum 1967).

⁵ Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477.

⁶ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

⁷ *Mohtarma Benazir Bhutto* (n 1).

⁸ *Katz v United States* 389 US 347 (1967).

⁹ *Manzoor Ahmad* (n 3).

¹⁰ *M D Tahir Advocate v Director, State Bank of Pakistan* CLD 2004 Lahore 1680.

Yar a warrantless police raid of "secret information" was said to infringe upon the inviolability of the home unless subject to judicial examination.¹¹ In *Taufiq Bajwa vs. CDGK*, a "structural intrusion" into visual privacy a neighbouring boundary wall allowing observation into a private residence was found to be actionable under Article 9's right to life.¹² Under Article 25, everyone has the right to equality before the law and equal protection of the law, which applies when a law or practice is applied unequally against specific groups, journalists, or political dissenters in the absence of any face-to-face justification. The fair-trial guarantee of Article 10A does not apply to substantive matters, however, it kicks in when evidence, gathered by surveillance, is used in criminal proceedings because there is a tension between the fairness it guarantees and evidence that has been gathered in an uncertain legal manner. Article 19A is also relevant to the constitutional entitlement to privacy in the face of state surveillance.¹³ It ensures that all citizens have access to information on public matters, subject to regulation and lawful and reasonable restrictions. This right has two meanings in the digital surveillance context, first to ensure transparency on the legal basis, institutional protection, and governance of the surveillance systems, and, second, to ensure a careful balance between disclosure and the potential impact on legitimate national-security or investigative interests. While Article 19A does not provide a clear right to know in all contexts, it fortifies the constitutional arguments for transparency, accountability and public oversight of state institutions that have intrusive data collection powers. However, there is no Supreme Court case law on digital surveillance. They were all identified via telephone interception using analogue or early digital telecommunications systems, not the integrated biometric platform of the NADRA. There were no algorithmic facial recognition, which have only recently come into existence, yet before the 21st century and Safe City networks, or any of the other leading authorities to emerge from the network. There is no reported supreme court decision that has considered whether the Bhutto principle of unconstitutionality of surveillance without statutory and judicial authorisation applies to bulk biometric collection, real time facial recognition matching or cross database search between NADRA, FIA and provincial Safe City authorities. The big doctrinal blind spot this article fills is the constitutional principle itself, however; it is in existence, but it has not been applied to the present modern system of surveillance.

3. Pakistan's Expanding Surveillance Architecture

3.1. Safe City Projects

Today, the Punjab Safe Cities Authority in Lahore, the Islamabad Safe City Project, run by the Pakistan Capital police in collaboration with the Chinese company Huawei, and similar systems in Peshawar and Karachi use the combination of dense CCTV and video analytics that can identify number-plates and, in newer deployments, facial features matched to NADRA's identity database. The systems have been argued for mostly in terms of terrorism prevention and urban policing requirements since the 2014 Army Public School attack, and their deployment has continued with no specific legislation on how long cameras can be retained, what the access logs will look at, or when facial-recognition patterns can be used as investigative leads, not just as evidence to

¹¹ *Ghulam Hussain v Additional Sessions Judge, Dera Allah Yar* PLD 2010 Quetta 21.

¹² *Taufiq Bajwa v CDGK* 2010 YLR 2165.

¹³ Article 19A of the Constitution of the Pakistan 1973

corroborate. There are no codes of practice in the public interest for deployment of Safe City authorities in Pakistan like the codes of practice in place for the equivalent deployments in the United Kingdom for biometric and surveillance cameras.

3.2. NADRA

Under the National Database and Registration Authority Ordinance 2000, NADRA has developed a biometric database containing fingerprints, photographs and family tree information of the entire registered population, and serves as the backbone of identity verification for almost all other government databases.¹⁴ Under section 26 of the Ordinance, the Registrar (NADRA) can request any user or feeder agency (which now includes law-enforcement agencies, banking institutions and telecom companies) to provide information for cross-verification, while section 22 requires feeder agencies to provide their own information to the Registrar upon request.¹⁵ While it is true that according to NADRA's public legal notices, biometric data is not shared with third parties for anything other than identity verification. It is not even subject to a statutory data-protection standard, but is only protected by internal policy, is quite significant when the database is used thousands of times a day by external agencies for verification purposes. This is on top of the Digital Nation Pakistan Act 2025, passed on 29 January 2025, which sets up the Pakistan Digital Authority and a National Digital Commission (NDC) to create an "inter-operable" data exchange layer. Which is deliberately designed to support inter-agency data flows among NADRA, the Pakistan Telecommunications Commission (PTA), and the State Bank and other regulators.¹⁶ In stark contrast, section 29 of the Act states that no decision made or action taken under the Act shall be questioned by any agency or challenged in any court or tribunal. Further, that no injunction shall be granted against such decisions or actions, which excludes judicial review exactly from the institution now tasked with rule-making in relation to cross-agency data sharing at national scale.

3.3. FIA/NCCIA Investigations

Previously, the FIA's Cyber Crime Wing carried out digital forensics phone extraction, social-media evidence gathering and cybercrime investigation. But amendments made under PECA 2025 have introduced a new National Cyber Crime Investigation Agency (NCCIA) which holds the same search, seizure and disclosure powers as the current wing of the FIA under sections 33 and 34 of the act.¹⁷ The powers, explored in detail in next chapter below, allow content and traffic to be acquired from service providers, on principle with court warrants, although with a number of exceptions for urgent warrantless acquisition.

3.4. Telecommunications Surveillance

Requirements of the Pakistan Telecommunication (Re-organization) Act 1996 (PTRA) and the provisions of the SIM-verification offence in PECA, enforce the biometric SIM registration, which means that every mobile phone connection is linked to a NADRA verified identity. In addition, the telecom operators shall maintain the call detail and traffic data and shall allow the lawful

¹⁴ National Database and Registration Authority Ordinance 2000, ss 3, 9.

¹⁵ *ibid* ss 22, 26.

¹⁶ Digital Nation Pakistan Act 2025 (Act No I of 2025), enacted 29 January 2025.

¹⁷ Prevention of Electronic Crimes (Amendment) Act 2025, establishing the National Cyber Crime Investigation Agency in place of the FIA Cyber Crime Wing; Prevention of Electronic Crimes Act 2016, ss 33–34.

interception on following the ministerial or judicial orders. Section 54 of the PTRa also provides for the simple Executive notification for interception in the interest of national security which has been apparently used to allow the ISI to intercept calls and messages without going through the IFTA 2013 warrant process.¹⁸

3.5. Other Government Databases

Gradually, passport, immigration, excise, health and education records are being tied into a single identity layer, which is anchored on NADRA, with the Digital Nation Pakistan Act now making them a national policy. The net result is one single profile under 2025 Finance Act changes which provides FBR with powers to get into any citizen's internet usage profile even browsing history from suspected tax fraud cases.¹⁹ The profile as a whole is not regulated by a single statute and is not subject to independent review of cross-agency access.

4. Existing Legal Framework

Pakistan's surveillance mechanisms are found in at least five statutes, all of which have been formulated for other purposes, with none of them designed to mesh with the others.

The Constitution provides the only cross-cutting standard for the dignity and privacy guarantee in Article 14 but, as chapter 3 demonstrated, it has never been used by the superior courts explicitly to address digital or biometric surveillance.

On paper, Pakistan's most stringent surveillance legislation is the Investigation for Fair Trial Act, 2013 (IFTA). It restricts itself to "scheduled offences" (primarily those of a 'terrorist' nature) and demands an actual judicial proceeding. The applicant agency (ISI, the three services' intelligence agencies, the Intelligence Bureau or police) must first obtain the authorisation from the Interior Minister before turning to a High Court judge who hears the case in chambers and can issue a warrant of surveillance or interception valid for up to 60 days.²⁰ This is the nearest Pakistani law comes to pre-authorization by the judiciary. But by design, it does not encompass the normal criminal investigation, does not involve sharing of data by NADRA or facial recognition as in Safe City and warrants itself are issued ex parte without adversarial testing and without an independent post-hoc audit like the Investigatory Powers Commissioner's Office in the UK.

The Prevention of Electronic Crimes Act 2016 (PECA), on the other hand, incorporates both judicial and executive authorisation within a single piece of legislation. Under section 33, a court may issue a warrant for search or seizure based on reasonable grounds. While section 34 provides that content data is only disclosable from a service provider with a court warrant (upon recorded reasons). Section 32 requires that the data and other telecom and internet service providers retain traffic data for at least one year and provide this data to investigators only upon the issuance of a warrant by a court (upon recorded reasons).²¹ Section 39 provides for the real-time collection of communications data on application to a "Court of competent jurisdiction," but section 31 expedites preservation and acquisition of data to the exclusion of a judicial hearing. Once made, it

¹⁸ Pakistan Telecommunication (Re-organization) Act 1996, s 54.

¹⁹ Finance Act 2025 (amendments empowering the Federal Board of Revenue to access internet-usage data in suspected tax-fraud cases).

²⁰ Investigation for Fair Trial Act 2013, s. 6–11, 14.

²¹ Prevention of Electronic Crimes Act 2016, ss 32–34.

is just a formality for the Pakistan Telecommunication Authority to notify the court, and therefore not a judicial power at all but a power of the Authority.

Under the Pakistan Telecommunication (Re-organization) Act 1996, lawful interception is possible via PTA-licensed operators while, as mentioned, it also allows for interception by national security agencies under section 54, outside any warrant process through which the bulk interception of telephones in Pakistan is believed to be conducted.²² The NADRA Ordinance 2000 regulates the data collection and sharing between agencies under the 'feeder agency' mechanism outlined above, but does not include a data-minimisation principle, a purpose limitation clause in terms of which the data subject can be bound and a separation of the regulator from the agency, its oversight is within its own structure. All these instruments have been superseded by the Digital Nation Pakistan Act 2025 which has been written as the architecture for cross-agency data exchange, and a separate Personal Data Protection Bill, with investigative and corrective powers like those of a civil court, which remains as of mid-2026, not yet enacted.²³

The practical problems of these six instruments, which overlap and are confused, are the following: IFTA provides judicial pre-authorisation but only for a limited range of offences. PECA provides judicial warrants that are burdened with clauses allowing urgent-acquisition exceptions and the PTTRA has no judicial role at all for national-security interception. While NADRA has no external oversight of its own data sharing, and the 2025 digital-governance framework designed to coordinate all of the above expressly precludes judicial review of its own decisions. There is no law that even requires a proportionality analysis before using biometric or facial-recognition surveillance, no law that provides a right to notification after surveillance, no law that gives any body apart from the executive the authority to audit compliance across agencies the very safeguards Part 6 argues Article 14 already implicitly demands.

5. Judicial Oversight and a Constitutional Proportionality Framework

As evident from the above discussion, the privacy legislation in Pakistan does not offer a holistic framework on when a violation of privacy is constitutionally permissible. Each statute has its own interpretation of authorisation and many types of data collection and inter-agency information sharing don't fall under the same umbrella of prior judicial review. The principle must be able to motivate against various forms of surveillance and legislation if the constitutional right to privacy is to have any traction. The article proposes such a principle as emerging from a proportionality principle, emerging from the idea of article 14 in combination with the articles 4, 9, 19 and 25 of the Constitution.

5.1. Legality

Legality should be the first criterion. There has to be a clear and easily understood legal basis, for any and all major encroachments on privacy. It would not be appropriate for executive agencies to be allowed to obtain general administrative powers that enable them to glean information from other sources where their exercise has a substantial impact upon constitutionally protected interests. Surveillance legislation needs to define with reasonable clarity the situations in which surveillance can be implemented, the powers of those who can do it, the kinds of information that

²² Pakistan Telecommunication (Re-organization) Act 1996, s 54.

²³ Personal Data Protection Bill (Pakistan), as at mid-2026 not yet enacted.

can be collected, the period for which it can be authorised to be collected and the purpose for which it may be collected.

5.2. Legitimate Aim

The aim of the surveillance has to be a legitimate governmental goal. The privacy rights of an individual may be sufficiently curtailed by carefully constrained interference with privacy in the fulfillment of national security, prevention and investigation of serious crime, protection of public safety and other constitutionally legitimate ends. But the presence of a valid purpose should not be enough to make the surveillance constitutional. The requirement for a legitimate governmental purpose is a precondition for intrusive surveillance, but it does not give unlimited rights to collect and retain personal data.

5.3. Necessity and Rational Connection

The government must establish that the proposed surveillance is "rationally connected" to the purpose and is actually "necessary" for that purpose. The justifications should be stronger the more intrusive the surveillance will be. A record of the locations visited, biometric data, communications or behaviour profile might prove to provide significantly more information than the interception of a specific communication. The assessment of the constitutionality therefore should rely on the nature, scale and duration of the intrusion, not all forms of surveillance.

5.4. Least Restrictive Means

There should also be some consideration to whether the legitimate purpose could be accomplished in a less intrusive way. The aim of surveillance should not be collected indiscriminately or in bulk unless it is necessary to achieve the investigative goal. In the same way, it should be necessary to provide further justification when allowing information to be retained or used for a different purpose, for a defined investigative purpose. Biometric and algorithmic surveillance pose a special challenge for this requirement as large groups of people may be impacted without being suspected of any specific actions or offences.

5.5. Proportionality *Stricto Sensu*

Finally, the cost and harm to individual rights must be weighed against the public good or harm from surveillance. Considerations for this assessment should be the sensitivity of the information, the number of people involved, length of surveillance, potential misuse, access to safeguards, and the impact on privacy, dignity and freedom of expression. Surveillance that focuses on a serious and specific threat may be proportionate if it is accompanied by adequate safeguards, but surveillance that is indiscriminate and based on mass amounts of personal information may need a significant justification.

5.6. Procedural Safeguards

The principle of substantive proportionality must be supported by a principle of procedural safeguards. Where the surveillance is particularly intrusive, prior authorisation from an independent judicial body should normally be required. The authorising body must have adequate information to assess whether the statutory requirements, the legitimate aim, the necessity and proportionality requirements have been met. There are situations that might justify exceptions to the rule of time limits in emergencies for a period of time where substantial harm would result if the exception were not granted, but exceptions should be limited and reviewed expeditiously by the court.

5.7. Independent Oversight and Post-Surveillance Remedies

A system of oversight cannot be guaranteed without judicial approval. Independence of institutional review of surveillance agencies is also needed to review warrants, retention, access to data, sharing restrictions etc. After surveillance, individuals should be notified, except for narrowly drawn exceptions which are vital to the protection of ongoing investigations. Remedies should be available when there is an absence of legal, proper and appropriate surveillance or when surveillance is carried out in an unauthorized manner. Put together, the provisions offer a constitutional structure that can evolve to account for new technologies, without needing a new constitutional rule for every new surveillance technology. The framework would enable Pakistani courts to examine the traditional interception of telephones, biometric databases, facial recognition, location tracking and cross-agency data sharing based on a common set of constitutional principles without overlooking the different levels of intrusion.

6. Comparative Constitutional Analysis

In India the Supreme Court of India, in Justice K.S. Puttaswamy (Retd) v Union of India, in a nine-judge bench unanimously ruled that the right to privacy is a fundamental right. An intrinsic part of the fundamental right to life and personal liberty as guaranteed under Article 21 of the constitution of India and also forms part of the fundamental right to freedom guaranteed under Part III of the Constitution expressly overruling the earlier contrary authorities of M.P. Sharma and Kharak Singh.²⁴ The Court established a three-part test for the lawfulness of every state measure which interferes with privacy, namely, the test of legality, the test of legitimate aim, and the test of proportionality, and that the right to informational privacy is the right to control over one's information. Puttaswamy is instructive for Pakistan not because of Article 21's "life and liberty" and Article 14's "dignity and privacy of home" are identical in their interpretation, but because both the articles started with narrower meaning of the right. Both protecting the life and liberty of Pakistanis and the dignity and privacy of home for Indians respectively but the rights have been read in a wide manner by both the Pakistani and the Indian Courts. It was merely a doctrinal step in Mohtarma Benazir Bhutto case, but did not take any further step in the digital and biometric era in Pakistan. In United Kingdom the Investigatory Powers Act 2016 answers the judicial-authorization question to the conflicting answer of Pakistani law. It has a "double-lock" feature, meaning that a warrant for the most intrusive powers interception, equipment interference and bulk acquisition requires two approvals: from the Secretary of State, followed by an independent Judicial Commissioner who must approve the necessity and proportionality of the decision.²⁵ Where the situation is urgent, the action can be done without giving prior approval but with a compulsory prior notification to a Judicial Commissioner who may cancel the authorization. The Act also established a single Investigatory Powers Commissioner's Office to monitor, on a

²⁴ *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1, overruling *M.P. Sharma v Satish Chandra* AIR 1954 SC 300 and *Kharak Singh v State of UP* AIR 1963 SC 1295.

²⁵ Investigatory Powers Act 2016, ss 19, 23 (interception warrants and Judicial Commissioner approval).

continuous basis, the use of authorised powers by more than 600 public organisations, precisely the independent systemic oversight role which is lacking from all Pakistani surveillance laws.²⁶ It's a similar thought that's picked up on in Pakistan's IFTA 2013, which requires High Court permission but whose next step is never to follow up on the use.

In United States, In *Carpenter v United States*, the U.S. Supreme Court ruled that the government's warrantless access to historical cell-site location information from a suspect's wireless provider must be conducted with a warrant based on probable cause under fourth amendment.²⁷ The Court explained that the location records are no longer collected by the government, but rather are compiled and maintained by third parties and generately created by cell phone users, often in an automated, unconscious manner, over a span of years. The importance of Carpenter case for Pakistan is that the method, not the text, of the case is relevant; the Court focused on the nature of digital data its comprehensiveness, its automatic production, its ability to reveal associations and habits as the basis for an enhanced level of protection, not where the data is physically located. It's the same logical step that Pakistani courts haven't taken yet in extending Bhutto's telephone-tapping principle to NADRA's biometrics and Safe City's facial-recognition algorithm.

Table 1: Constitutional and Institutional Safeguards against State Surveillance: A Comparative Analysis

Jurisdiction	Constitutional privacy basis	Judicial warrant for surveillance	Independent oversight body	Citizen remedy
India	Art 21 (Puttaswamy, 2017)	Proportionality test, case-by-case	Emerging (data protection authority pending)	Constitutional writ
United Kingdom	Statutory (IPA 2016)	Double-lock: Secretary of State + Judicial Commissioner	Investigatory Powers Commissioner's Office	Investigatory Powers Tribunal
United States	Fourth Amendment (Carpenter, 2018)	Probable-cause warrant for CSLI/digital records	Judicial suppression remedy, no standing inspectorate	Exclusionary rule; civil suit
Pakistan	Art 14 (Benazir B., 1998) untested on digital surveillance	Only for IFTA-scheduled offences; PECA warrants with 24-hour exception; none for NADRA/PTRA national-security interception	None independent of executive	Constitutional petition only, post facto

7. Reforming Pakistan's Surveillance Laws

The gaps mapped above have four key reforms flowing from them. First, Pakistan must have a comprehensive Data Protection Act that finally makes the long-delayed Personal Data Protection

²⁶ Investigatory Powers Act 2016, Part 8 (Investigatory Powers Commissioner and Judicial Commissioners).

²⁷ *Carpenter v United States* 138 S Ct 2206 (2018).

Bill into law. Also with a Commission independent of the executive, not a data governance that is covered by an ouster clause in the Digital Nation Pakistan Act. Second, IFTA's judicial-warrant concept ought to be extended beyond scheduled crimes of terror to encompass data-sharing requests for NADRA, facial-recognition deployment in Safe City and interception in PTRa by the national security services, as most surveillance currently takes place without a judge's involvement. Third, Pakistan should put in place an independent body, similar to IPCO, with statutory powers to conduct after-the-warrant inspection of the powers of agencies rather than just to approve the warrant and then to come out with a public report and report to Parliament. Fourthly, there needs to be special legislation regarding facial recognition and biometric matching, a technology which is being deployed quickly through Safe City systems but has not been addressed by any legislation in Pakistan to introduce accuracy requirements, retention periods or restrictions on its uses.

8. Conclusion

Today, Pakistan has high capacity of surveillance, low constitutional protections and insignificant judicial oversight of its use. This article argues that principle emerging from *Mohtarma Benazir Bhutto* case should be extended to contemporary forms of digital surveillance particularly when such surveillance interferes without statutory and judicial authorization. As it is already in Article 14, interpreted in *Benazir Bhutto's* context and within the frameworks of Articles 4, 9 and 25, and yet it has never been tested against the biometric database of NADRA, the facial recognition technology of Safe City or the cross-agency data architecture of the Digital Nation Pakistan Act. In different constitutional lexica, it is India's *Puttaswamy*, the United Kingdom's double-lock, and the United States' *Carpenter*, who all demonstrate that legitimate national-security and law-enforcement goals can have a place in the realms of legality, necessity, proportionate restrictions and independent judicial oversight. The state's increasingly powerful ability to spy on its citizens is not enough to justify national security; a constitutional democracy is the one in which the state's ability to watch its citizens is matched by the citizens' capacity to know when they are being watched and to question it when the watching is illegal.

Bibliography

- Mohtarma Benazir Bhutto and Others v President of Pakistan* [PLD 1998 SC 388].
Ms Shehla Zia v WAPDA PLD 1994 SC 693.
Manzoor Ahmad v The State [1990 MLD 1488 LHC].
 Alan Westin, *Privacy and Freedom* (Atheneum 1967).
 Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477.
 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).
Mohtarma Benazir Bhutto (n 1).
Katz v United States 389 US 347 (1967).
Manzoor Ahmad (n 3).
M D Tahir Advocate v Director, State Bank of Pakistan CLD 2004 Lahore 1680.
Ghulam Hussain v Additional Sessions Judge, Dera Allah Yar PLD 2010 Quetta 21.
Taufiq Bajwa v CDGK 2010 YLR 2165.
 National Database and Registration Authority Ordinance 2000, ss 3, 9.

Digital Nation Pakistan Act 2025 (Act No I of 2025), enacted 29 January 2025.
Prevention of Electronic Crimes (Amendment) Act 2025, establishing the National Cyber Crime Investigation Agency in place of the FIA Cyber Crime Wing; Prevention of Electronic Crimes Act 2016, ss 33–34.
Article 19A of the Constitution of Pakistan 1973.
Pakistan Telecommunication (Re-organization) Act 1996, s 54.
Finance Act 2025 (amendments empowering the Federal Board of Revenue to access internet-usage data in suspected tax-fraud cases).
Investigation for Fair Trial Act 2013, s. 6–11, 14.
Prevention of Electronic Crimes Act 2016, ss 32–34.
Pakistan Telecommunication (Re-organization) Act 1996, s 54.
Personal Data Protection Bill (Pakistan), as at mid-2026 not yet enacted.
Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, overruling *M.P. Sharma v Satish Chandra* AIR 1954 SC 300 and *Kharak Singh v State of UP* AIR 1963 SC 1295.
Investigatory Powers Act 2016, ss 19, 23 (interception warrants and Judicial Commissioner approval).
Investigatory Powers Act 2016, Part 8 (Investigatory Powers Commissioner and Judicial Commissioners).
Carpenter v United States 138 S Ct 2206 (2018).