



PRIVACY BEYOND SECRECY: ARTICLE 14, DIGITAL INFERENCE AND THE CONSTITUTIONAL LIMITS OF ALGORITHMIC SURVEILLANCE IN PAKISTAN

Mohammad Adnan

Bachelor of Laws (LLB) Session 2017-2020 & Master in History (M.A) session 2018-2020. Both from university of the Punjab Lahore.

Email: adnanzarin7@gmail.com

Maham Chuhdary

LLM. (PULC)

Permanent Faculty member (Lincolns Inn Law College)

Email: cmaham050@gmail.com

Zeeshan Amjad

Department: Punjab University Law College

Email: zeeshanamjad757@gmail.com

Abstract

Constitutional privacy law was developed when surveillance usually meant entering a home, intercepting a communication, or obtaining information an individual attempted to keep secret. Digital surveillance complicates that model. Governments can increasingly combine location records, traffic data, biometric identifiers, facial-recognition matches, device information and other digital traces. Individually, some of these data points may be public, legally accessible, or only weakly private. Aggregated and analysed, however, they may reveal intimate information about movements, relationships, associations and routines that the individual never expressly disclosed. Pakistan's Article 14 protects dignity and, subject to law, the privacy of home. Pakistani jurisprudence has already moved beyond a purely spatial conception of privacy, but it has not developed a general doctrine for sensitive knowledge generated by aggregation and algorithmic inference. This article argues that the unresolved problem lies between private information and public facts: digital systems can generate private knowledge from data that is not individually secret. It proposes a Constitutional Inference Principle and a four-stage framework - Collection, Aggregation, Inference and Consequence. The framework does not treat artificial intelligence or surveillance as inherently unconstitutional. It requires constitutional scrutiny to intensify when aggregation materially increases informational resolution, analysis derives sensitive conclusions, and those conclusions produce significant governmental consequences. The article grounds the proposal in Article 14, Pakistani case law and surveillance statutes, while using comparative law only as an analytical aid. It concludes that constitutional privacy in an algorithmic State must govern not only what government collects, but what government is able to make of what it collects.

I. From Interception to Inference: The New Constitutional Privacy Problem

Traditional surveillance has a familiar structure. The State enters a home, installs a listening device, intercepts a telephone conversation, opens correspondence, or extracts information from a personal device. Something regarded as private exists, and government attempts to obtain it. Article 14 of the Constitution reflects this historical concern by declaring the dignity of man and, subject to law, the privacy of home inviolable. Yet digital surveillance can operate without crossing a physical threshold. A camera records a face in public; telecommunications systems retain traffic data;



identity systems hold biometric information; public records reveal addresses; and analytical tools can connect these fragments. The constitutional problem is therefore no longer only what private information the State obtained. It is also what private knowledge the State created from information it possessed. This distinction matters because the informational significance of a dataset can change after collection. One location point may reveal little; a year of location history may reveal routines. One communication record may be mundane; a longitudinal contact graph may reveal relationships. One camera image may show presence; persistent identity-linked observations may reconstruct movement. The harm, if any, may emerge from pattern reconstruction rather than the secrecy of a single datum.

Pakistan's constitutional text supplies an important starting point but not a complete answer. Article 14 expressly mentions the privacy of home, yet the Supreme Court's decision in *Mohtarma Benazir Bhutto v President of Pakistan* treated telephone tapping and bugging as violations of Articles 9 and 14. More recently, the Lahore High Court in *Muhammad Rehmat Ullah v State* held that information a person wishes to keep secret in a mobile phone cannot simply be extracted without consent or lawful process, and that necessary investigative retrieval requires permission of the concerned court with strict regard to constitutional privacy. These authorities show that privacy cannot be reduced to physical walls. The difficulty appears when information is not secret at the source. In *Justice Qazi Faez Isa v President of Pakistan*, the Supreme Court majority rejected a privacy claim regarding property records open to public inspection and distinguished *Benazir Bhutto*. That limitation is important. Article 14 should not convert every personal fact into confidential information. But the case does not answer what happens when many accessible facts are combined to generate an intimate behavioural portrait that no single record contains.

This article calls that problem the aggregation paradox: information may be individually non-private yet collectively privacy-revealing. The proposed Constitutional Inference Principle responds to that paradox. State access to individual data points should not, merely because each point was lawfully obtained or publicly observable, automatically place every aggregate or algorithmically derived inference outside Article 14. Where aggregation or analysis materially reconstructs intimate aspects of an identifiable person's life, associations, movements or behaviour, constitutional scrutiny should extend to the inferential process and its use. The proposal is deliberately limited. It does not create ownership over facts, a right to anonymity in every public place, or a constitutional prohibition on data analysis. It asks when informational transformation becomes sufficiently intimate and consequential to require justification. The article operationalises that inquiry through four stages: Collection, Aggregation, Inference and Consequence. Lawfulness at Collection remains essential, but it does not necessarily settle every later stage.

II. Reconstructing Article 14 for Digital Privacy

The Constitutional Inference Principle must be anchored in Pakistani constitutional law rather than technological anxiety. Article 14 combines two ideas: dignity of the person and privacy of the home. A strictly spatial interpretation would make constitutional privacy progressively weaker as personal life migrates to networks, cloud services and digital devices. The better approach is not to erase the words "privacy of home," but to read them alongside dignity and the jurisprudence concerning technologically mediated intrusion. *Benazir Bhutto* is foundational because the constitutional wrong was not confined to physical entry. Telephone tapping and electronic bugging allowed government to penetrate private life through technology. The Islamabad High Court has



subsequently relied on Benazir Bhutto when addressing allegations of mass surveillance, observing that freedom of speech also includes speaking without the State prying on private conversations and treating warrantless mass surveillance as raising grave constitutional concerns. These decisions do not establish inferential privacy, but they reject the proposition that Article 14 becomes irrelevant once observation occurs through infrastructure rather than a doorway.

Dignity supplies the conceptual bridge. Privacy protects a measure of freedom from unjustified governmental reconstruction of personal life. Persistent digital observation can convert a constitutional subject into an object of continuous analysis. A human observer may see a person enter a building; a networked system may record the event, connect the face to an identity, retain the history, combine it with other observations and calculate patterns. The first observes an event. The second can construct a profile. Article 14's dignity language gives Pakistani courts an indigenous reason to ask whether that difference matters. Qazi Faez Isa remains the necessary counterweight. The majority held that no confidentiality attached to property records legally open to the public and therefore accessing those records was not covert surveillance or an invasion of privacy. The Constitutional Inference Principle accepts that starting point. It does not transform a public property record into a secret. It instead distinguishes the privacy status of source information from the constitutional significance of informational transformation. Accessing one public fact and constructing an intimate profile from thousands of facts are analytically different acts.

Muhammad Rehmat Ullah supplies the clearest bridge to informational privacy. The Lahore High Court recognised that a mobile phone can contain a vast range of personal intellectual and communicative activity and held that private information cannot be extracted except with consent or as law directs. It further required court permission where retrieval is essential to criminal investigation. The judgment therefore establishes that digital form does not strip information of constitutional significance and that legal process can mediate informational intrusion. These authorities permit four categories to be distinguished. Spatial privacy asks where the State may intrude. Communications privacy asks what it may intercept. Informational privacy asks what personal data it may access. Inferential privacy, proposed here, asks what sensitive knowledge it may reconstruct or derive from data it possesses. Pakistani courts have not recognised the fourth category as a freestanding right. The article therefore presents it as a doctrinal development, not settled law.

International law provides a useful interpretive parallel. Article 17 of the International Covenant on Civil and Political Rights protects privacy, family, home and correspondence against arbitrary or unlawful interference. Human Rights Committee General Comment No 16 states that gathering and holding personal information in computers and data banks must be regulated by law and that individuals should have means to ascertain, correct or eliminate unlawfully processed personal data. These materials cannot rewrite Article 14, but they reinforce the proposition that modern privacy is not synonymous with domestic space. The central move can therefore be stated precisely: lawful collection should not always exhaust constitutional analysis. Algorithmic surveillance introduces post-collection transformation. Information lawfully obtained for one purpose may later be combined with other sources, used to generate sensitive classifications, retained as a profile, or relied upon for coercive action. The legality of acquisition answers an indispensable question; it does not necessarily answer every later one.



The distinction between device privacy and networked information also sits within Pakistan's broader electronic-transactions and telecommunications environment.

III. Pakistan's Surveillance Architecture: Regulating Collection, Not Inference

Pakistan does not operate in a legal vacuum. The Investigation for Fair Trial Act 2013 creates a statutory architecture for specified covert surveillance and interception, including judicial warrant procedures. Its existence reflects an important constitutional proposition: investigative usefulness does not itself settle legality; procedure mediates power. Yet the Act is primarily technique-oriented. A warrant may answer whether government may obtain specified information without fully answering what sensitive knowledge may later be generated from it. PECA 2016 is another central component. The current official text contains procedural powers relating to preservation, retention, search, seizure and real-time collection. Section 32 requires service providers to retain specified traffic data for at least one year, subject to statutory conditions and lawful production. Retention can be indispensable to investigation, but it also creates the raw material for retrospective behavioural analysis. A statutory duty to preserve data is not necessarily a legislative determination that every inference later derivable from that data is constitutionally unrestricted.

Section 39 is particularly revealing. It permits a court, on application by an authorised officer, to order real-time collection for a specific criminal investigation where statutory conditions are met. The application must identify the information sought and include measures to ensure that the privacy of other users and third parties is maintained. The order is initially limited in duration. These safeguards demonstrate that Pakistani law already recognises necessity, specificity and third-party privacy at the acquisition stage. The regulatory mismatch arises downstream. Contemporary systems can combine information obtained under separate powers or for separate purposes. Identity administration, telecommunications, camera systems and criminal-investigation records may each have distinct legal foundations. When interoperable, however, their combined informational capacity may exceed what any individual legal regime contemplated. The constitutional unit may become the informational ecosystem rather than the isolated database.

Safe City infrastructure illustrates the problem without requiring an assumption that every Pakistani system performs every technically possible function. Official parliamentary material has discussed facial-recognition functionality in Safe City contexts and the use of biometric verification technologies. Facial recognition can serve legitimate public-safety purposes. The constitutional concern is functional escalation: a camera can observe, record, identify, track, connect observations across locations, and potentially support behavioural analysis. These functions should not be treated as constitutionally identical merely because they begin with an image captured in public. Biometrics raise a similar purpose-transformation issue. Information collected to answer “is this person who he claims to be?” may later help answer “where is this person?” or “is this the person recorded by a surveillance system?” The secondary use may be legitimate, but the legality of the first collection should not automatically justify every later use. Purpose limitation therefore has constitutional relevance even if it is more familiar as a data-protection principle.

Pakistan's wider data-governance architecture also remains incomplete. As of October 2026, the Ministry of Information Technology and Telecommunication continues to list the Personal Data Protection Bill May 2023 as a draft rather than an enacted comprehensive statute. The Ministry lists the Data Governance Policy 2026 as draft, while the National Artificial Intelligence Policy was approved in July 2025. Policy development is significant, but policy and constitutional law perform



different functions. Article 14 asks what public power may constitutionally do to the person through information. Recent Pakistani scholarship confirms that the broad problem of digital privacy is no longer novel. A 2025 article proposes an Article 14 AI-surveillance test built around legal clarity, legitimate purpose, necessity, data minimisation and independent oversight. Other recent scholarship argues for informational privacy and proportionality in relation to State surveillance, examines AI-driven policing and privacy concerns, and surveys enforcement of privacy rights in Pakistan. This literature narrows the defensible contribution of the present article. Its novelty cannot be that surveillance requires safeguards. The distinctive claim is that constitutional analysis must identify the inference itself as an object of scrutiny and follow information through Collection, Aggregation, Inference and Consequence.

The underlying concern also reflects the longstanding international prohibition on arbitrary interference with privacy.

IV. Comparative Lessons Without Constitutional Transplantation

Comparative law can illuminate the aggregation problem, but foreign doctrine should not control Article 14. Three bodies of jurisprudence are particularly useful because each contributes a different analytical insight. First, *Carpenter v United States* concerned historical cell-site location information and rejected a simplistic treatment of extensive digital location records as ordinary business records. The United States Supreme Court emphasised the revealing nature of a comprehensive chronicle of physical movements. The useful lesson for Pakistan is not the Fourth Amendment's reasonable-expectation test. It is the recognition that aggregation can alter the constitutional character of information. One public observation and a long-term reconstructed movement history are not necessarily equivalent. This is sometimes described as a mosaic effect. Each observation is a tile; the assembled pattern reveals the picture. The concept fits the proposed inference principle because it focuses on the informational whole. It does not require a numerical rule under which the ninety-first observation suddenly becomes unconstitutional. It requires courts to ask whether accumulation materially changed what government could know.

Second, *Justice K.S. Puttaswamy (Retd.) v Union of India* recognised privacy as constitutionally connected to dignity, liberty and informational privacy. The Indian Supreme Court stressed that privacy attaches to the person and is not surrendered merely because an individual is in a public place. Pakistan should not import *Puttaswamy* as binding doctrine, but its connection between dignity and informational personhood is analytically relevant because Article 14 itself expressly protects dignity. *Puttaswamy* also helps explain why algorithmic classification can matter. Government databases do not merely store facts; analytical systems can construct institutional representations of persons. Such representations may be accurate, incomplete, outdated or wrong. When they materially influence State action, privacy intersects with the individual's ability to contest how government has informationally constituted her.

Third, European surveillance jurisprudence contributes an institutional insight. In *Big Brother Watch and Others v United Kingdom*, the European Court of Human Rights emphasised end-to-end safeguards in bulk interception and the increasing degree of intrusion as surveillance moves through different stages. The value of this reasoning for Pakistan is not the transplantation of Article 8 ECHR. It is the proposition that surveillance legality can depend on architecture - authorisation, selection, handling, retention, supervision and remedies - rather than only proof of abuse after the event. These comparisons yield three principles. From *Carpenter*: aggregation matters because the



whole can reveal substantially more than its components. From Puttaswamy: dignity can support protection of informational personhood beyond physical secrecy. From European jurisprudence: systematic surveillance requires safeguards across its lifecycle. Together they support, but do not determine, a Pakistan-specific doctrine.

The limits of comparison are equally important. Article 14 contains distinctive text; Pakistan's statutory surveillance architecture differs from foreign systems; and courts should not constitutionalise the entirety of foreign data-protection law. Comparative authorities are therefore persuasive analytical resources only. The ultimate rule must be justified through Pakistan's Constitution, domestic jurisprudence and institutional context. European Article 8 provides the textual setting for that jurisprudence, while *Centrum för rättvisa* similarly emphasises safeguards in bulk surveillance. American location and device cases beyond *Carpenter* also illustrate concern with technologically enhanced reconstruction and digital depth.

V. The Constitutional Inference Framework

The framework contains four stages: Collection, Aggregation, Inference and Consequence. Its purpose is graduated constitutionalism rather than prohibition.

At Collection, courts ask how government obtained the information, under what authority, for what purpose, whether consent or judicial permission was required, and what safeguards applied. Directly private communications and device contents ordinarily demand stronger protection than facts openly observable in public. Existing statutes and case law remain controlling. If Collection is unlawful, later analytical sophistication cannot cure the defect. At Aggregation, the question changes: did combining information materially increase the State's capacity to reconstruct private life? Five factors are useful. Duration asks how long the combined record extends. Breadth asks how many categories of information are connected. Continuity distinguishes episodic from persistent observation. Linkability asks whether separate information is reliably tied to one identifiable person. Revelatory capacity asks whether the combined dataset discloses substantially more than its components. Enhanced scrutiny should arise when these factors produce a substantial and reasonably foreseeable increase in informational resolution.

Purpose also matters. Data lawfully collected for traffic administration, identity verification or another administrative purpose may later be valuable to law enforcement. Secondary use is not automatically unconstitutional, but substantial purpose transformation can require renewed justification. The greater the departure from the original purpose and the greater the new intrusion, the stronger the constitutional case for additional authority or safeguards. At Inference, the court asks what government derived from the data. An observation that a person entered a building differs from an inference about why she entered. A record of repeated communications differs from a conclusion that the participants share criminal activity. Enhanced Article 14 scrutiny should focus on sensitive personal inferences concerning intimate relationships, religious practice, political or associational activity, health-related behaviour, habitual movements, private communications networks, identity or similarly significant aspects of private life.

The proposed trigger is this: Article 14 scrutiny should intensify where governmental analysis derives sensitive personal information not directly observed or expressly contained in the source data and materially expands State knowledge of an identifiable person's private life. This does not make every inference constitutionally protected. Routine administrative inference remains possible. The threshold turns on sensitivity, informational expansion and governmental use. Reliability is



critical because algorithmic outputs often express probability rather than fact. A facial-recognition result may be a similarity score; network analysis may identify statistical centrality; a behavioural model may produce a risk classification. Government should distinguish observed fact, algorithmic match, statistical correlation and substantive inference. Where a sensitive inference may produce serious consequences, an accountable institution should be able to evaluate the quality of the underlying data, relevant limitations, confidence, contradictory information and the extent of human verification.

Meaningful human review should become more demanding as consequences increase. Human presence is not equivalent to human judgment. A reviewer should have enough information and authority to identify uncertainty, consider contrary material, reject the automated recommendation and assume responsibility for the decision. At Consequence, courts ask what government did with the inference. Anonymous statistical analysis presents a different problem from an investigative lead; an investigative lead differs from enhanced surveillance; and those uses differ again from an inference materially contributing to search, detention, arrest or another serious exercise of State power. The framework therefore adopts an Escalation Principle: the more intimate the inference and the more serious the governmental consequence, the stronger the required justification, reliability, verification, documentation and review.

Not every aggregation or inference should require a warrant. Additional judicial authorisation becomes more compelling where several factors converge: persistent monitoring of an identifiable individual; combination of multiple datasets producing substantially increased insight; highly sensitive inference; material purpose change; and intended use for intrusive surveillance or coercive action. Emergency powers can accommodate immediate threats, but urgency should postpone safeguards rather than erase accountability. Proportionality remains part of the analysis but is not the article's novelty. The contribution is to apply proportionality across the informational lifecycle. A collection measure can be proportionate while a later inference or use is not. Courts should consider lawful objective, rational connection, less intrusive alternatives, breadth, duration, retention, sharing and safeguards appropriate to the sensitivity of the output.

The framework also proposes inferential minimisation. Conventional data minimisation asks whether more data than necessary were collected. Inferential minimisation asks whether government generated more sensitive knowledge than reasonably necessary for the legitimate purpose. If an investigation requires knowing whether a person was present at one place on one date, reconstructing a year of movement may require additional justification even if the underlying records lawfully exist. Retention should distinguish source data from derived profiles. An unverified inference should not become permanent digital suspicion merely because storage is inexpensive. Sensitive profiles should be reviewed for continuing relevance, reliability and investigative connection. Auditability is equally important: systems capable of materially affecting rights should preserve enough information to identify data sources, purpose, analytical method, significant output, reviewer and consequential action, subject to legitimate confidentiality.

The four-stage judicial test can therefore be stated succinctly. Collection: was the information lawfully obtained under safeguards proportionate to its nature? Aggregation: did combination materially increase the State's capacity to reconstruct private life, and was it connected to a lawful purpose? Inference: did analysis generate sensitive conclusions not directly contained in source data, and were they sufficiently reliable and verified? Consequence: how was the inference used,



what effect did it have, and were safeguards proportionate to that effect? The framework is also consistent with privacy scholarship emphasising multiple forms of privacy harm, contextual integrity, re-identification risk, limits of consent, quantitative accumulation and data-intensive policing.

VI. Stress-Testing the Framework in Pakistani Surveillance Contexts

A facial-recognition match provides the simplest example. Assume a camera captures a person in public and authorised software compares the image against a database of wanted persons. Collection may involve relatively limited privacy. Aggregation is narrow. The inference is a possible identity match. If the result merely prompts human verification and further lawful inquiry, the constitutional burden is modest. If an automated match alone becomes the principal basis for detention, reliability and verification requirements increase sharply. A facial-recognition alert can justify investigation more readily than it can, standing alone, justify coercion.

Now change the facts. Historical camera records are searched to reconstruct an individual's movements over months. Even if every image was captured in public, Aggregation now changes the informational character of the material. Duration, continuity and linkability are substantial. If the system identifies regularly visited locations and classifies their meaning, analysis moves from movement reconstruction to sensitive inference. Visibility at each moment does not necessarily imply constitutional indifference to permanent visibility across time. Telecommunications metadata illustrates the same distinction. Lawfully obtained traffic data may reveal communication patterns without exposing content. Months of records can identify networks; software can identify central nodes; investigators may infer relationships. But mathematical network centrality is not the same as culpable association. Family members, lawyers, businesses and innocent contacts can occupy prominent positions in a communication network. Association inferred from metadata should therefore not automatically become guilt.

Cross-database biometric matching raises purpose transformation. Assume biometric information was collected for identity administration and law enforcement seeks to compare surveillance footage against that database. The secondary use may be legitimate, but the relevant question is what legal authority permits it and what safeguards govern the change in purpose. The original legality of identity collection should not automatically answer the surveillance question. A harder scenario is the algorithmic suspect. Instead of beginning with a named person, a system processes information concerning a broad population, combines location and communication indicators, and assigns risk scores. One individual becomes a suspect only because the model selected her. The framework distinguishes algorithmic suspicion from legally sufficient suspicion. A score may generate further inquiry; it should not automatically constitute the legal basis for intrusive action.

False matches demonstrate why Consequence matters. Collection and aggregation may both be lawful, but an inaccurate facial-recognition inference accepted without meaningful verification can lead to wrongful detention. The constitutional injury arises downstream. Conversely, false negatives can distort investigations. The objective is not to presume algorithms are hostile to rights but to prevent uncritical reliance on automated outputs. Sensitive locations provide another illustration. Raw coordinates are geographical facts. When combined with knowledge that a location is a medical facility, place of worship, political organisation or intimate residence, geography can become sensitive information. The inference arises from combining where a person went with what the place means.



Seriousness of purpose also changes proportionality. A credible imminent threat of terrorism may justify highly intrusive, targeted analysis when lawfully authorised and appropriately verified. The same months-long cross-database reconstruction used for a minor regulatory offence would present a very different balance. Technology is not constitutional or unconstitutional in the abstract; purpose, scope and consequence matter. Finally, networked systems process information concerning innocent persons. PECA section 39's express concern for the privacy of other users and third parties provides a domestic statutory foothold for minimisation. Automated systems can process innocent-person data at a scale impossible for traditional human investigation. Inferential minimisation therefore asks how much of an individual's life government actually needs to reconstruct to answer the legitimate investigative question.

VII. Institutions, Remedies and the Constitutional Minimum

Recognising inferential privacy would accomplish little if doctrine operated only after irreversible harm. Algorithmic surveillance is often invisible to the person affected. Institutional design is therefore part of substantive protection. Judicial authorisation should remain central where intrusion is greatest. PECA section 39 already demonstrates a model in which a court considers specificity, necessity, duration and third-party privacy before real-time collection. Where an application seeks persistent cross-database analysis rather than one stream of information, the authorising institution should understand the analytical scope contemplated: categories of data, period, purpose, expected sensitive inferences, proposed use and safeguards.

Oversight cannot end when permission is issued. Datasets expand, analytical systems change, and information may outlive the investigation that justified it. Auditability bridges secrecy and accountability. Legitimate investigations cannot always be transparent, but an authorised reviewer should be capable of reconstructing what information was processed, why, what significant inference emerged, whether human verification occurred and what governmental action followed. Technical complexity should not defeat judicial review. Courts need not become software laboratories, but they should be able to obtain independent technical assistance when a materially consequential inference cannot otherwise be evaluated. Experts explain capability, uncertainty and limitations; judges decide legality.

Where algorithmically generated information enters adjudication, Article 14 may intersect with Article 10A's guarantee of fair trial and due process. A person should be able, subject to lawful confidentiality restrictions, to challenge materially consequential inferences: identity, accuracy of source information, misleading context, reliability, and the significance attributed to an automated output. Contestability does not require advance notice during covert investigation, but a system in which consequential classifications can never be meaningfully questioned raises serious due-process concerns. Correction and retention are also important. An erroneous association can be reused across systems. Sensitive unverified inferences, false matches and classifications that have lost relevance should be subject to correction, segregation, deletion or periodic review as appropriate. Cheap storage is not itself a constitutional reason for permanent governmental memory. Parliament is better placed than courts to design detailed regulation. A future statutory framework should address legal authority for intrusive analytical uses, purpose limitation, cross-database integration, sensitive inferences, meaningful human verification, retention of derived profiles, audit records, independent supervision, third-party data, correction and remedies. Risk calibration is essential: a traffic-management algorithm should not be regulated identically to a system used to



select persons for coercive investigation. Courts, however, need not wait for a perfect code to identify constitutional floors. Those floors should include lawful authority; legitimate objective; proportionality between informational intrusion and purpose; heightened justification where aggregation substantially reconstructs private life; reliability and meaningful verification before serious consequences; and enough accountability to permit review.

Technology should receive neither constitutional immunity nor constitutional hostility. Scale, persistence, searchability, interoperability and inference matter because they change governmental capability. At the same time, algorithms can improve accuracy, speed and public safety. The Constitutional Inference Principle is technologically neutral: it asks whether the informational power exercised by government is accompanied by safeguards proportionate to its effect on the person.

VIII. Conclusion: When Information Becomes Power

The deepest change produced by algorithmic surveillance is not simply that the State possesses more data. It is that contemporary analytical systems can make existing data mean more than they meant when separately collected. A camera records presence; a telecommunications record identifies contact; a database supplies identity; a location record supplies geography. Combined over time, they can reconstruct a life. Pakistani jurisprudence already supplies the beginnings of a broader privacy doctrine. Benazir Bhutto shows that constitutionally significant surveillance is not confined to physical entry. Qazi Faez Isa provides an essential limitation: information does not become constitutionally private merely because it concerns a person. Muhammad Rehmat Ullah shows that digital information can attract Article 14 protection and that lawful process matters. The unresolved space lies between these propositions: what happens when accessible or lawfully acquired information becomes deeply revealing only after computational combination?

The Constitutional Inference Principle answers that the legality of obtaining information should not necessarily exhaust constitutional inquiry where State systems transform that information into substantially more intimate knowledge about an identifiable person. Collection asks whether government lawfully obtained information. Aggregation asks whether combination materially increased informational resolution. Inference asks whether analysis generated sensitive conclusions beyond the source data and whether those conclusions are reliable. Consequence asks what government did with that knowledge and whether safeguards were proportionate to its effect. This approach preserves legitimate surveillance. Serious criminal investigation, public safety and national security can justify intrusive measures. Facial recognition and metadata analysis can generate valuable leads. But constitutional justification should intensify as surveillance moves from observation toward reconstruction and from reconstruction toward coercive consequence.

The framework also explains why the public/private binary is increasingly insufficient. Digital systems can create private knowledge from public facts. The constitutional question is therefore not merely whether a person concealed each datum. It is whether governmental aggregation and inference produced an informational portrait sufficiently intimate and consequential to engage dignity and privacy. Pakistani courts have not yet recognised a freestanding right to inferential privacy. This article does not claim otherwise. It proposes a development of Article 14 grounded in domestic doctrine, the dignity text, the structure of existing surveillance law and the changing capabilities of the State. Parliament should provide detailed rules for algorithmic surveillance,



integration, retention, auditability and contestability. Courts should establish the constitutional boundary beyond which technological capability cannot substitute for legal justification.

In the algorithmic State, constitutional privacy must govern not only what government collects, but what government is able to make of what it collects.

References

Constitution of the Islamic Republic of Pakistan 1973.

Prevention of Electronic Crimes Act 2016 (Pakistan).

Investigation for Fair Trial Act 2013 (Pakistan).

Electronic Transactions Ordinance 2002 (Pakistan).

Pakistan Telecommunication (Re-organization) Act 1996.

Qanun-e-Shahadat Order 1984 (Pakistan).

Mohtarma Benazir Bhutto v President of Pakistan and others, PLD 1998 SC 388.

Justice Qazi Faez Isa v President of Pakistan, PLD 2021 SC 1.

Muhammad Rehmat Ullah v State, 2024 PCrLJ 1 (Lahore High Court); also reported as 2023 LHC 4087.

Islamabad High Court, Writ Petition No 2758 of 2023, judgment/order concerning mass surveillance and constitutional privacy.

International Covenant on Civil and Political Rights 1966, art 17.

Universal Declaration of Human Rights 1948, art 12.

UN Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy) (1988).

UN Human Rights Council, The Right to Privacy in the Digital Age, relevant resolutions.

Office of the UN High Commissioner for Human Rights, reports on The Right to Privacy in the Digital Age.

European Convention on Human Rights, art 8.

Carpenter v United States, 585 US 296 (2018).

United States v Jones, 565 US 400 (2012).

Riley v California, 573 US 373 (2014).

Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

Big Brother Watch and Others v United Kingdom, App nos 58170/13, 62322/14 and 24960/15 (ECtHR Grand Chamber, 25 May 2021).

Centrum for rattvisa v Sweden, App no 35252/08 (ECtHR Grand Chamber, 25 May 2021).

Roman Zakharov v Russia, App no 47143/06 (ECtHR Grand Chamber, 4 December 2015).

S and Marper v United Kingdom, App nos 30562/04 and 30566/04 (ECtHR Grand Chamber, 4 December 2008).

Jamil MS and others, "Privacy of Home to Privacy-by-Design: Article 14 of the Pakistani Constitution in the Age of AI Surveillance" (2025) 3(1) International Research Journal of Arts, Humanities and Social Sciences 279-293.

Elif MU, "State Surveillance without Safeguards: Constitutional Limits on Digital Monitoring in Pakistan" (2026) Social Science Review Archives.

Soomro SA, Kalhor HB and Gujjar M, "AI-Driven Policing in Pakistan: Potential Pitfalls, and Privacy Concerns" (2025) Pakistan Social Sciences Review.



- Idrees RQ, Hussain N and Jameel MS, “The Recognition and Enforcement of Right to Privacy in Pakistan: Challenges and Way Forward” (2026) 4(3) Pakistan Journal of Social Science Review 377-383.
- Butt MF and others, “The Right to Privacy in the Age of Surveillance: Legal Protections in Pakistan” (2025).
- Solove DJ, “A Taxonomy of Privacy” (2006) 154 University of Pennsylvania Law Review 477.
- Solove DJ, “Privacy Self-Management and the Consent Dilemma” (2013) 126 Harvard Law Review 1880.
- Solove DJ, Understanding Privacy (Harvard University Press 2008).
- Nissenbaum H, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).
- Ohm P, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization” (2010) 57 UCLA Law Review 1701.
- Gray D and Citron DK, “The Right to Quantitative Privacy” (2013) 98 Minnesota Law Review 62.
- Ferguson AG, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (NYU Press 2017).
- Richards NM, “The Dangers of Surveillance” (2013) 126 Harvard Law Review 1934.
- Richards NM, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (Oxford University Press 2015).
- Kerr OS, “The Mosaic Theory of the Fourth Amendment” (2012) 111 Michigan Law Review 311.
- Citron DK and Pasquale F, “The Scored Society: Due Process for Automated Predictions” (2014) 89 Washington Law Review 1.
- Brayne S, Predict and Surveil: Data, Discretion, and the Future of Policing (Oxford University Press 2020).
- Lyon D, Surveillance Studies: An Overview (Polity 2007).
- Lyon D, The Culture of Surveillance: Watching as a Way of Life (Polity 2018).
- Cohen JE, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice (Yale University Press 2012).
- Cohen JE, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press 2019).
- Wachter S and Mittelstadt B, “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI” (2019) 2 Columbia Business Law Review 494.
- Barocas S and Selbst AD, “Big Data’s Disparate Impact” (2016) 104 California Law Review 671.
- Kroll JA and others, “Accountable Algorithms” (2017) 165 University of Pennsylvania Law Review 633.
- Pasquale F, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015).
- Zuboff S, The Age of Surveillance Capitalism (PublicAffairs 2019).
- Gellert R, The Risk-Based Approach to Data Protection (Oxford University Press 2020).
- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, as modernised by Protocol CETS No 223).
- Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024).



European Union, General Data Protection Regulation, Regulation (EU) 2016/679.

European Union, Artificial Intelligence Act, Regulation (EU) 2024/1689.

OECD, Recommendation of the Council on Artificial Intelligence (2019, updated 2024).

UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

Ministry of Information Technology and Telecommunication, Pakistan, Personal Data Protection Bill May 2023 (Draft).

Ministry of Information Technology and Telecommunication, Pakistan, National Artificial Intelligence Policy 2025.

Ministry of Information Technology and Telecommunication, Pakistan, Data Governance Policy 2026 (Draft).

National Assembly of Pakistan, parliamentary materials concerning Safe City, biometric verification and facial-recognition technologies.