



RESEARCH ARTICLE

The Right to Privacy in the Digital Age: Article 17 ICCPR and Comparative Institutional Protection in the United Kingdom, Canada, Australia, India and Pakistan

Waheed Rafiq¹

Mirza Khurram Baig²

¹ Deputy District Public Prosecutor, Punjab Prosecution Department, Pakistan. E-Mail: aliabasssial@gmail.com

² Head of Law Department, Multan University of Science and Technology, Pakistan. E-Mail: Mkb5729@gmail.com

ARTICLE HISTORY

Received **11-09-2025**

Accepted **28-11-2025**

Published **30-12-2025**

KEYWORDS

right to privacy, digital surveillance, data protection, facial recognition, artificial intelligence, proportionality, comparative human rights, Pakistan, India

CORRESPONDING AUTHOR

Waheed Rafiq

aliabasssial@gmail.com



<https://doi.org/10.68740/91>

ABSTRACT

This article explores the extent to which international human rights standards protect privacy from contemporary digital surveillance and data processing. It uses doctrinal and comparative legal analysis to assess Article 17 of the International Covenant on Civil and Political Rights and related standards in relation to four operational variables: legality and foreseeability, necessity and proportionality, independent oversight, and effective remedy. The report compares the UK, Canada, Australia, India and Pakistan, with a particular focus on bulk and targeted surveillance, private-sector data processing, facial recognition and automated decision-making. The analysis finds the international standard to be relatively stable at the level of principle but uneven in practical application. General Comment No. 16 already requires the adoption of legislative and other measures to ensure protection against interference by State authorities and private actors. Subsequent United Nations materials and regional jurisprudence have developed more detailed safeguards. The reach of these principles is a matter of domestic institutions: courts, regulators, warrant mechanisms, data-protection statutes, notification duties and remedies can turn international norms into enforceable constraints, while broad exemptions, weak oversight and fragmented remedies can make the same norms largely declaratory. The article's main contribution is an institutional comparison of the domestic 'hooks' through which Article 17 and related privacy standards gain practical force. It concludes that effective digital privacy protection depends not on a new statement of the right alone but on legally foreseeable powers, independent oversight, meaningful remedies and technology-neutral regulation that can reach both State and private processing.

1. INTRODUCTION

Privacy is a fundamental human right that is challenged by technologies that increase the scale, speed and opacity of collection. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interference with privacy, family, home and correspondence and requires that such interference be provided by law. The text was written before the advent of social media, cloud computing, large-scale biometric technology and modern artificial intelligence, but the legal concepts of lawfulness, arbitrariness and protection of the law can still be applied to these technologies. The central research problem is not, therefore, whether privacy exists as a right, but whether the legal institutions for the enforcement of that right can limit technologically enabled interference.

The practices examined are in two overlapping areas, state surveillance and processing in the private-sector. State surveillance includes interception, metadata acquisition, interference with equipment, intelligence sharing and facial recognition deployment. Private processing includes platform profiling, data brokering, biometric identification and use of personal data to train or run automated systems. General Comment No. 16 is particularly important because the Human Rights Committee pointed out that article 17 protects against interference by State authorities and natural or legal persons and that it requires States to adopt legislative and other measures. The treaty therefore creates an obligation for the State to protect privacy, while the way in which that obligation translates into duties for companies and public authorities is a matter for domestic law (Human Rights Committee, 1988).

The comparison covers the UK, Canada, Australia, India and Pakistan. These jurisdictions share important common-law features but differ in constitutional structure, data protection legislation, regulatory institutions and surveillance controls. This comparison is not a ranking of national populations or political systems. This is a comparison of legal reception, of how a common international privacy norm connects to domestic constitutional rights, statutes, regulators, warrant mechanisms and remedies.

The article argues that international privacy standards are institutionally contingent but normatively significant. Article 17 provides a general framework of legality, non-arbitrariness, reasonableness and protection of law. General Comment No. 16 also provides for regulation of personal information held by public and private bodies (Human Rights Committee, 1988). But the real effect of a norm depends on domestic institutions that can authorise, review, regulate, investigate, and redress any interference. The analytical claim is modest but testable: international privacy standards gain more practical purchase where they are linked to a clear domestic legal basis, proportionality review, independent oversight and an effective remedy.

The article goes on to say: Section 2 reconstructs the international norm. Sections 3-5 cover State surveillance, private-sector processing, and facial recognition and artificial intelligence. Sections 6-10 apply the same analytical framework to the five jurisdictions. Section 11 compares the results through the institutional-hook thesis and discusses the implications of the two heuristic figures and tables that are retained. Section 12 End.

1.1 Research Question

The key question is the extent to which international human-rights standards provide privacy protections against modern digital surveillance and data-processing practices. For the purposes of this study, effectiveness is an analytical concept, not a legal test. It is assessed on the basis of four variables: (1) whether the interference is based on a clear and reasonably foreseeable legal basis; (2) whether necessity and proportionality are reviewable in a meaningful way; (3) whether the interference can be authorised, supervised or challenged by an independent oversight body; and (4) whether there is an effective remedy against both public and private processing. They draw on

relevant international and comparative jurisprudence. They are not put forward as a single universal four-part treaty test.

1.2 Literature Review, Research Gap, Contribution, Objectives and Methodology

There are a number of strands of debate opened up by the existing literature. The first concerns the adaptability of Article 17 to technological change and the extent to which privacy should be understood through autonomy, identity, dignity and control of information. Recent academic literature on surveillance and artificial intelligence argues that digital surveillance affects not only secrecy but also the environment in which people construct and perform identity (Matar & Murray, 2025). The second strand focuses on comparative data protection and the relationship between constitutional privacy and statutory regulation, including the burgeoning India-Pakistan literature (Ali & Hussain, 2024). The third relates to the practical regulation of biometrics. Here, the need, proportionality, transparency and purpose limitation of regulatory and judicial decisions are increasingly being put to the test. Fourth, institutional design: whether a right has an independent regulator, a warrant mechanism, a court willing to scrutinise novel technologies and a remedy capable of reaching private processors. The research gap is located at the intersection of these strands. Much of the scholarship is either jurisdiction-specific or focused on a single technology or legal instrument. This article, by contrast, compares the institutional pathways by which an international privacy norm becomes practically enforceable in five common-law jurisdictions. Its contribution is not to argue that Article 17 itself creates identical domestic remedies. It is to identify a recurrent institutional mechanism. International standards are most operative when domestic law provides a predictable legal basis, a proportionality forum, independent oversight and an effective remedy. The aims are to state the content of Article 17 and its digital-age elaborations; to examine their application to surveillance, commercial processing, biometrics and automated decision-making; to compare the five systems through legislation, judgements and regulators; to identify the domestic institutions that operationalise international standards; and to develop a legally grounded account of institutional conditions for effective privacy protection. The method is doctrinal and comparative in nature. Secondary commentary is less preferred than primary materials. The central evidence consists of treaty texts, treaty-body materials, regional judgements, constitutions, statutes, domestic judgements and official regulatory decisions. These primary materials are interpreted and contextualised with soft-law instruments and academic literature. The temporal cut-off is 27 September 2026. The study is documentary, not empirical, and therefore cannot ascertain actual privacy outcomes in the population; the absence of reported litigation is not used as evidence that surveillance or biometric processing does not occur. Figures 1 and 2 are retained at the author's instruction and are heuristic organising devices and not statistically-measured national scores.

2. INTERNATIONAL HUMAN RIGHTS NORMS

2.1 Article 17 ICCPR

Article 17 provides for the right to protection against arbitrary or unlawful interference with privacy, family, home or correspondence and the right to protection against unlawful attacks on honour and reputation. The Human Rights Committee has said that 'unlawful' means that an interference must have a basis in law, whereas 'arbitrariness' goes beyond formal legality and requires reasonableness in the circumstances. General Comment No. 16 thus connects legality with substantive reasonableness and proportionality (Human Rights Committee, 1988).

General Comment No. 16 is dated but foundational. It deals specifically with electronic surveillance, wire-tapping and recording of conversations and makes provision for the regulation of the collection and holding of personal information by public authorities and private bodies. It

also recognises the rights of access, correction and elimination of false or unlawfully obtained files (Human Rights Committee, 1988). The subsequent evolution of digital privacy should thus be seen as an application and extension of an existing norm, not the creation of an entirely new right.

2.2 The Digital-Age Acquis

Privacy in the digital era has subsequently been taken up by the United Nations in General Assembly resolutions and human-rights reports. Resolution 79/175 of the General Assembly, adopted on 17 December 2024, reaffirms the right to privacy and emphasises the importance of lawfulness, legitimate aims, necessity and proportionality in technology-related measures (United Nations General Assembly, 2024). While these resolutions are useful interpretive and policy documents, they are not legally binding, as is the ICCPR. The article thus considers them as indicators of international normative development rather than independent treaty obligations.

Comparative jurisprudence is particularly well developed for article 8 of the European Convention on Human Rights. *Big Brother Watch and Others v. the United Kingdom* and *Centrum för Rättvisa v. Sweden* demonstrate that bulk interception is not, in itself, incompatible with Article 8 but that legal safeguards, authorisation and oversight are central to compatibility. The cases are binding within the ECHR system. For Canada, Australia, India and Pakistan they are comparative persuasive materials, not controlling law. This is an important distinction as the ICCPR and the ECHR have different institutional and remedial regimes.

2.3 Positive Duties and Private Processors

Article 17 also imposes obligations on States to protect privacy from interference by natural and legal persons. General Comment No. 16 clarifies that the obligation applies to interferences originating outside State authorities and requires legislative and other measures to implement the prohibition (Human Rights Committee, 1988). This underpins national data protection laws, regulation, security obligations, rights of access and correction, breach rules and limitations on inappropriate biometric processing in modern language. That is not to say that Article 17 is a directly enforceable private tort against each company. The domestic legal system remains the main avenue for translating the State's protective obligation into enforceable duties.

3. STATE SURVEILLANCE

Modern State surveillance has moved from targeted interception to bulk acquisition, metadata retention, equipment interference, intelligence sharing and biometric identification. Article 17 does not prohibit intelligence activity per se. It requires interferences with privacy to be lawful and non-arbitrary, and to be accompanied by effective protection of the right. The legal-quality question is therefore key: does the legal framework define the scope of the power, the purposes for which it may be used, the categories of information affected, the authorising body, retention rules and mechanisms of review?

“Necessity and proportionality are not the same as legality. A power may be statutory but still arbitrary, if its exercise is unreasonable or disproportionate. In particular, independent authorisation and after-the-fact oversight are all the more important where the affected individual is not aware that surveillance has occurred. This institutional problem is exemplified by the European bulk-interception jurisprudence. General Comment No. 16 provides the framework for the ICCPR.

Another challenge is extraterritorial surveillance, where data flows across borders, but legal remedies are territorially organised. The international standard thus is better at identifying the need for lawful and non-arbitrary interference than at supplying a universal transnational remedy.

The comparative question is how domestic systems handle jurisdiction, standing, secrecy, intelligence sharing and review.

4. PERSONAL DATA AND PRIVATE-SECTOR PROCESSING

The bulk of personal information is held by private organisations, rather than intelligence agencies. The international human-rights obligation is implemented domestically through data-protection rules governing lawful bases, purpose limitation, data minimisation, security, retention, access, correction and accountability. General Comment No. 16 makes explicit the private-body dimension, such that contemporary data-protection statutes are relevant to the treaty analysis regardless of the companies are not parties to the ICCPR.

Biometric processing flags the issue. Facial images and biometric templates derived from them may be used for authentication, identification, loss prevention, policing or profiling. The issue of processing legality turns on the domestic statute under which it is conducted and the specific circumstances, including whether there is a lawful basis, whether the processing is reasonably necessary for the purpose, whether less intrusive means are available and whether affected persons are provided with adequate notice and remedies. The Clearview AI, Bunnings and Kmart cases offer useful comparisons as regulators and courts have been forced to apply general privacy statutes to technologies not expressly named in the original legislation.

5. FACIAL RECOGNITION AND ARTIFICIAL INTELLIGENCE

Facial recognition should be analysed as a family of technologies, not as a singular practice. Live facial recognition scans a crowd against a watchlist, retrospective recognition searches stored images and operator initiated recognition supports an investigating officer of a known person. These uses carry different risks of legal interference and of evidentiary issues. The judgement of the European Court in *Glukhin v. Russia* is particularly important as it directly addressed facial-recognition processing to identify and locate a peaceful protestor and identified violations of Articles 8 and 10 (European Court of Human Rights, 2023).

With AI, the problem goes from observation to inference. Automated systems can deduce characteristics, classify people, recommend intervention or make major decisions from data that a person did not provide for that purpose. The relevant legal questions are not only about transparency. These include the legal basis for processing, compatibility of purpose, accuracy, bias and discrimination, meaningful human involvement, contestability and remedies. Recent UK reforms show that rules for automated decision-making are themselves rapidly evolving, and Australian and Indian reforms are also evolving in stages. The comparison therefore considers AI as a stress test of the existing principles of legality and proportionality.

6. THE UNITED KINGDOM

The UK will combine Article 8 of the European Convention, which was incorporated into UK law by the Human Rights Act 1998, with the UK GDPR, the Data Protection Act 2018, the Investigatory Powers Act 2016 and the Data (Use and Access) Act 2025 by September 2026. Independent bodies include the Information Commissioner's Office and the Investigatory Powers Commissioner's Office. The framework is institutionally dense but its effectiveness is conditional on the interplay of statutory powers, oversight and guidance.

In *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, the Court of Appeal held that the use by the police of live automated facial recognition was not 'in accordance with the law' for Article 8 purposes in the circumstances of that case. The Court found shortcomings in the

legal framework concerning where the technology could be deployed and who could be put on watchlists. It also found a failure in relation to the Public Sector Equality Duty (Bridges, 2020). The ruling did not create a blanket statutory ban on facial recognition, but rather exemplifies how legality and foreseeability may operate as constraints on new forms of surveillance.

Thus the post-Bridges position is not that facial recognition is forbidden but that deployment must be accompanied by a legally sufficient framework and compliance safeguards. Official guidance on policing and regulation has continued to develop. The lesson for analytical purposes is that general power may sometimes be enough, if combined with sufficiently specific rules and safeguards, but the question of legality remains fact-sensitive.

Bulk interception is located within the statutory framework of the Investigatory Powers Act 2016. The European Court's jurisprudence has influenced the architecture of authorisation and oversight, while the UK legislation contains judicial-commissioner and warrant mechanisms. The key question of comparison is not whether the UK has surveillance powers – it obviously does – but whether the combination of statutory scope, authorisation, safeguards, oversight and remedies gives meaningful protection against arbitrary interference.

And the UK's data-protection regime changed materially in 2025–2026. The Data (Use and Access) Act 2025 altered the rules on significant automated decision-making and introduced safeguards including information about decisions, representations, human intervention and contestation. The ICO says the data-protection elements of the Act were in place by June 2026. The revised framework should therefore be read as part of the legal position in September 2026, rather than describing UK data protection only through the pre-2025 UK GDPR architecture.

7. CANADA

Canada protects privacy under section 8 of the Canadian Charter of Rights and Freedoms, and under federal and provincial privacy legislation. PIPEDA remains the primary federal private-sector law for commercial activities and the Privacy Act for federal public-sector information. In Canadian constitutional jurisprudence, reasonable expectations of privacy take a different route in public law and criminal law. The comparison thus differentiates constitutional search protection from statutory data governance.

Federal statutory reform is not over. The Protecting Privacy and Consumer Data Act, or Bill C-36, was tabled in the House of Commons on June 15, 2026. It is an omnibus bill proposing to replace Part 1 of PIPEDA with a new private-sector privacy statute and to establish a new institutional structure but it was still a bill at the September 2026 cut-off. It cannot therefore be said to be a law in force. I believe that the previous Bill C-11 and Bill C-27 should be treated as legislative history, not law.

One high-profile cross-border case is that of Clearview AI. In *Clearview AI Inc. v. British Columbia (Information and Privacy Commissioner)*, 2026 BCCA 67, the British Columbia Court of Appeal upheld the applicability of British Columbia's Personal Information Protection Act to the foreign facial-recognition company, and upheld the order of the Commissioner regarding the collection and use of facial data. The case demonstrates the ability of a provincial privacy regulator to reach a foreign technology company where the connection to the province is sufficiently significant. The BCCA decision should be qualified with that procedural status, as the leave application to the Supreme Court of Canada was live at the research cut-off in September 2026.

However, the Canadian system has nothing comparable to the UK's Investigatory Powers Act in a single federal statute. Intelligence and policing powers are distributed across statutes like the CSIS Act and Criminal Code provisions, as well as judicial warrant processes and privacy oversight. The issue is not whether Canada has safeguards, but whether its institutional architecture is more

distributed. That distribution can provide multiple paths to review, but it can also make the regulatory position less uniform.

Canada shows the significance of institutional pluralism. There are a number of potential venues for bringing privacy claims, such as the federal and provincial commissioners, courts and the Charter. Clearview also shows that processing online data isn't protected from domestic privacy law just because the processor is foreign. But since Bill C-36 remains before the legislature, the proposed federal reform should not be treated as settled law in the article.

8. AUSTRALIA

Australia does not have a federal constitutional bill of rights and privacy protection at the Commonwealth level is largely statutory and administrative, supplemented by State and Territory regimes. The Privacy and Other Legislation Amendment Act 2024 materially amended the Privacy Act 1988. A statutory tort for serious invasions of privacy commenced operation on 10 June 2025. The revised law provides for an additional judicial recourse within the regulatory structures of the Privacy Act. However, the tort contains wide exemptions including law-enforcement and intelligence activities.

“Retail facial recognition is a good example of regulatory evolution. The OAIC’s 2024 Bunnings determination found the retailer’s facial-recognition system to have serious privacy issues. But in February 2026, the Administrative Review Tribunal’s Guidance and Appeals Panel decided that the use of facial-recognition itself was within a permitted general situation, although it found breaches in relation to notification and privacy-policy requirements. The OAIC’s guidance published in July 2026 reflects the reasoning of the Tribunal and focuses on contextual assessment, necessity and proportionality. Kmart is a separate 2025 OAIC determination and was still under ART review at the September 2026 cut-off date.

The Australian example illustrates the way a technology-neutral statute can regulate biometric practices, without requiring a dedicated facial recognition Act. The hook of institutions is the regulator and the statutory principles, not a constitutional right to privacy. The statutory tort provides another avenue of redress, but its exemptions suggest that it should not be viewed as a panacea for every State-surveillance practice.

9. INDIA

In the *K.S.* case, the nine-judge Supreme Court laid down the decisive constitutional privacy framework in India. *Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1. The Court acknowledged privacy as a constitutional right tied to liberty, dignity and autonomy and developed proportionality as part of the framework for assessing restrictions. The decision is fundamental, but constitutional recognition and institutional enforcement are not the same thing.

India’s current statutory data-protection framework consists of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. The Rules were notified on 13 November 2025 but include provisions with staggered commencement dates. The Gazette provides that a number of substantive rules commenced 18 months after publication. Other provisions commenced earlier. The Data Protection Board of India has been constituted and its composition notified. The article should make a distinction between the institutional constitution and the date on which each of the substantive obligations shall become enforceable.

The Act includes important provisions regarding State processing and exemptions. Section 17 provides for exemptions in certain circumstances and changes the applicability of certain obligations to processing by the State. The question for the academy, therefore, is whether the

statutory architecture can be reconciled with the constitutional requirements of legality, legitimate aim and proportionality in *Puttaswamy*. This is a question of doctrinal analysis, not a determination that the statute itself is unconstitutional.

Aadhaar is an instance of the scale dimension of Indian digital governance, but claims of being the world's largest biometric system need to be substantiated by dated official evidence or left out. The position that is more defensible in law is that identity infrastructure involves the integration of multiple datasets and thus raises questions of purpose limitation, proportionality, security and institutional oversight. Those questions can be examined in the light of *Puttaswamy* and the current statutory scheme without having to resort to unsubstantiated numbers.

The relative absence of Indian facial-recognition litigation akin to *Bridges* or *Glukhin* should not be read to be indicative of the non-existence of such processing. It is more accurately an evidentiary limitation. The appropriate comparison is whether constitutional review, data-protection regulation, procurement rules and administrative law offer a practical way to challenge biometric deployments. The revised article accordingly avoids inferring prevalence or absence from reported case law alone.

10. PAKISTAN

Article 14 of the Constitution of Pakistan says that the dignity of man and, subject to law, the privacy of home shall be inviolable. As of 27 September 2026, Pakistan has not yet enacted a comprehensive personal-data-protection statute. The Senate record shows that the Personal Data Protection Bill, 2023, introduced as a private member's bill, was not passed or rejected by the committee, and was later disposed of/withdrawn. The draft Personal Data Protection Bill, 2023 is still listed as May 2023 on the website of Ministry of IT and Telecommunication. The article should therefore separate proposed legislation from enacted law.

The Prevention of Electronic Crimes Act 2016 was amended in 2025. The official amendment establishes the Social Media Protection and Regulatory Authority and the National Cyber Crime Investigation Agency and amends several provisions related to cybercrime and online content. These amendments matter to the digital-governance environment, but PECA is not a comprehensive personal-data protection law. Accordingly, the privacy analysis must focus on what PECA does regulate and what it does not regulate.

The most comprehensive primary human-rights source for the present analysis is the 2024 concluding observation on Pakistan by the Human Rights Committee. The Committee was concerned that PECA provided for excessive powers to access and retain personal data and to share it with foreign governments without sufficient judicial authorisation and oversight. It also referred to the Lawful Intercept Management System and other surveillance mechanisms, and called for a comprehensive data-protection law, compliance with the criteria of legality, proportionality and necessity in Article 17, independent oversight and effective remedies (Human Rights Committee, 2024). Allegations reported by civil-society organisations concerning surveillance capacity, database leaks or insider sales should be attributed to the sources and not presented as facts established by the judiciary.

Privacy is also relevant to security of collected information. Article 17 applies not only to the first collection of data but also to the State's obligation to protect personal data from unlawful interference and to provide effective remedies. So the Pakistani comparison is not merely about interception powers, but also about data retention, control of access, auditability, breach response and institutional accountability. Here one can see institutional gaps that result from the lack of an overarching data-protection statute.

Pakistan's case illustrates the difference between a constitutional privacy guarantee and a working privacy system. The constitutional language is Article 14, PECA is the cybercrime and online-content rules, there are large datasets from telecommunications and identity institutions, and the Human Rights Committee has identified specific concerns under Article 17. The key comparative question is therefore not whether Pakistan has privacy law, but whether its existing legal and institutional mechanisms provide the foreseeability, proportionality, independent oversight and remedy required for effective protection.

11. COMPARATIVE DISCUSSION

Six patterns emerge on comparison. First, constitutional recognition does not, in and of itself, determine practical protection. India has a strong constitutional privacy doctrine, but statutory implementation is pending; Canada has Charter search protection and several privacy regulators; the United Kingdom has a dense statutory framework; Australia relies heavily on statutory and regulatory mechanisms; and Pakistan has constitutional protection but no enacted comprehensive data-protection statute. These are institutional differences descriptive not ranking of societies."

Second, regulators have been particularly visible in commercial biometrics. Bunnings, Kmart and Clearview demonstrate how general privacy statutes can be applied to facial-recognition practices even where the legislature has not enacted a technology-specific biometric statute. Third, police and intelligence surveillance presents a different institutional problem in that secrecy, national security and classified evidence can limit access to ordinary remedies. Bridges and the European mass surveillance cases demonstrate why legality and independent oversight are important.

Fourth, artificial intelligence creates a temporal problem. Data-protection law is increasingly incorporating safeguards for automated decisions, but statutory reform is still piecemeal and implementation is often incremental. The UK DUA 2025, Australia's reforms and India's DPDP framework are different ways of dealing with automated decision-making and institutional oversight. Fifth, the remedies are significantly different: regulatory orders, administrative penalties, declarations, exclusionary rules and private causes of action are not the same type of redress. Sixth, accordingly the same international norm can produce different practical effects according to the domestic hook on which it is invoked.

The central contribution of the comparison is the institutional-hook thesis. The practical consequences of a treaty norm are most consequential when four conditions coincide: a foreseeable legal basis, a forum capable of proportionality review, independent oversight, and an effective remedy. The conditions need not be identical in each jurisdiction. Instead, the comparison shows why the practical reach of Article 17 cannot be determined by the text of the treaty alone.

Temporal lag is a perennial institutional problem. Technologies can be put in place before legislators specify protections. Bridges with live facial recognition, Bunnings and Kmart in commercial retail, Clearview with the cross-border dimension and Pakistan's existing framework with the consequences of having surveillance and cybercrime legislation without a comprehensive data-protection statute illustrate this. International standards cannot prevent technological lag, but they can provide a legal vocabulary for courts and regulators to demand more-specific rules.

Remedies merit separate consideration also. Each of a regulator's order, a fine, a declaration, a private tort claim, and a judicial exclusionary remedy addresses a different harm. International standards for an effective remedy do not prescribe a particular universal remedial model. The comparative question is whether the available combination gives the affected person a real opportunity to challenge unlawful or arbitrary processing.

Table 1 is kept as an organising device. It maps institutional hooks across four jurisdictions and deliberately discusses Pakistan in the ‘text around it’. Table 2 compares recurring domestic shortfalls with international standards. Because the tables employ broad comparative formulations, they should be read in conjunction with the more qualified country analyses rather than as independently verified quantitative measures.

Feature	United Kingdom	Canada	Australia	India
Constitutional hook	HRA / ECHR Art. 8	Charter s. 8 search and seizure	No federal bill of rights; implied political communication limited	Art. 21 privacy as fundamental right (Puttaswamy)
Data-protection statute	UK GDPR + DPA 2018	PIPEDA + Privacy Act; Bill C-36 pending 2026	Privacy Act 1988 as amended 2024	DPDP Act 2023; Rules Nov. 2025
Surveillance statute	Investigatory Powers Act 2016	CSIS Act, Criminal Code warrants; no single IPA analogue	Telecommunications metadata; Assistance and Access Act	Sectoral + broad State exemptions in DPDP
Facial recognition case	Bridges [2020] EWCA Civ 1058	Clearview (BCCA 2026); no federal FRT Act	Bunnings / Kmart OAIC determinations	Aadhaar and Pegasus litigation; no Bridges equivalent
Independent regulator	ICO + IPCO	OPC + provincial commissioners	OAIC	Data Protection Board of India (new)

Figure 1 is preserved as provided in original draft. Its numerical values are not empirical measures of privacy protection, but heuristic composite scores. The article does not say that 78, 64, 70, 58 or 32 are objectively measured national levels. They are a visual shorthand for the author’s comparative assessment of legal leverage. An appendix should contain the coding rules and weights themselves, to allow for a reproducible journal version.

Figure 2 is retained in its original form. Its percentages are author-estimated shares of the protective work attributed to different legal tools and are not to be interpreted as statistical observations. The comparative argument is based on the doctrinal analysis rather than on the numerical proportions shown in the figure.

12. CONCLUSION

The answer to the research question is conditional. International human-rights standards offer a resilient normative framework for privacy but their practical efficacy is highly dependent on domestic institutional mechanisms. Article 17 provides for protection against arbitrary and unlawful interference and, as General Comment No. 16 clarifies, requires States to adopt legislative and other measures to prevent interference by both public authorities and private actors. Subsequent UN texts and comparative jurisprudence under Article 8 have developed safeguards as to legality, necessity, proportionality and oversight.

The five jurisdictions show distinct institutional trajectories. The UK has combined Article 8 with comprehensive statutory regulation and independent oversight, and the current law cannot be understood without reference to the Data (Use and Access) Act 2025. Canada combines Charter protection, federal and provincial privacy regulators and developing federal legislative reform; Australia shows a technology-neutral statute and regulator’s ability to deal with biometric processing and now has a statutory tort, though the significant exemptions remain. India has a strong constitutional privacy doctrine and a new data-protection framework that is being operationalised. Phased implementation and State-processing provisions, however, mean that there is a need for continued doctrinal scrutiny. Pakistan has privacy protected by the constitution and laws against cybercrime but, as the Human Rights Committee noted in 2024, it does not have the comprehensive data-protection and independent oversight framework needed to address contemporary surveillance concerns.

Practice / What Art. 17 / Art. 8 require / Typical internal shortfall

Practice	What Art. 17 / Art. 8 require	Typical domestic shortfall
Bulk interception & metadata	Clear law, necessity, proportionality, independent authorisation and oversight	Mandates written for an earlier internet; oversight thinner than collection power
Live facial recognition	Foreseeable rules on where, whom and why; equality assessment	Common-law police powers plus guidance, not a dedicated statute
Commercial biometrics	Lawful basis, transparency, purpose limitation, deletion of non-matches	Consent buried; retail FRT treated as loss-prevention first
AI profiling	Human review of significant decisions; bias testing; explainability	Automated-decision rules arriving late and thin
Cross-border transfers & spyware	No end-run around domestic warrants by buying foreign tools	Export and procurement of spyware weakly policed
State databases (ID, tax, SIM)	Purpose limitation and security; access logs; redress for leaks	National ID systems leak; insider sale of records

The comparative finding is thus institutional, not just textual. International standards are more effective when they are tied to a predictable legal basis, meaningful proportionality review, independent oversight and an effective remedy. That is not to say every jurisdiction needs the same institutions, or a new global privacy treaty. This calls for domestic mechanisms to implement international standards both ahead of and after intrusive technologies are deployed.

The main reform implication is accordingly practical. States should ensure that substantial powers for biometric and automated processing have a clear legal basis, defined purposes, safeguards, independent review and accessible remedies; private-sector biometric processing should be subject to lawful-basis, transparency, proportionality and security requirements; and data-protection regimes should include effective supervision of State as well as private processing. These are proposals stemming from the comparative results and not claims that Article 17 necessitates one single statutory model. The main contribution of this article is to show why the institutional pathway from an international right to an individual remedy itself constitutes an important object of comparative legal research.

Figure 1 is not to be interpreted as a moral ranking of peoples. It is a sketch of legal leverage: constitutional text, data statute, surveillance oversight, biometric case law. The United Kingdom scores high because the statute book is fat. Australia scores high because the commissioner has been happy to treat retail recognition as a privacy event. Canada is in the middle due to the strength of the Charter and the age of the federal commercial statute. Because of the broad State exemptions in the new Act, India sits lower than Puttaswamy's reputation would suggest. The reason Pakistan is lowest is because the data bill is still a bill and the surveillance apparatus is not hypothetical. Figure 2 is making the same point, in a different shape. In Pakistan, much of the available protection consists of residual case law and gap. In the United Kingdom a large proportion is statutory. That is the identity of the set in the comparison.

12. SUMMARY

International human-rights standards protect privacy against modern digital surveillance and data-processing practices only insofar as domestic institutions will carry them. Still the right text is article 17. It prohibits arbitrary and unlawful interference. It needs a law that is not a blank cheque. It needs protection from the police, as well as from private processors. Digital-age resolutions and the European bulk-interception cases have updated the grammar of that text. Facial recognition and AI haven't made grammar obsolete. They have made the need for deletion, foreseeability rules, necessity analysis and equality testing more apparent.

The five common-law systems illustrate the appearance of carriage. The UK shows that a serious Article 8 jurisdiction and a dense statute can still leave a biometric practice running on guidance. Canada demonstrates that a robust search doctrine cannot update a commercial privacy statute by itself. Australia shows that with a principled commissioner you can do international-standard work on private-sector biometrics without a bill of rights. India shows how a landmark constitutional holding can co-exist with a data statute that leaves the security State plenty of room for manoeuvre. Pakistan shows dignity language and an electronic-crimes act are not systems of privacy.

A better settlement would do four unglamorous things. It will put live facial recognition and similar biometric crowd-scanning on a dedicated statutory footing with watchlist rules, location rules and independent authorisation. It would complete the long-delayed commercial reforms in Canada and enact a real data protection law in Pakistan. It would limit State exemptions in India's new scheme until they pass a Puttaswamy proportionality hearing. It would treat automated significant decisions as searches and events of processing, rather than as neutral infrastructure. None of that needs a new Covenant article. It requires the political decision to use the article one one already has as a constraint on procurement and design, rather than as a paragraph for the national report to Geneva.

Until that decision is made, the honest answer to the research question is this. The standards do a good job of naming the wrong and arming courts and commissioners that already have a hook. They are no match for a government that has decided a crowd is a data set. In those institutions, in the five systems studied here and others like them, privacy in the digital era will be won or lost, and not in the next recital of Article 17.

REFERENCES

- Ali, M. I., & Hussain, K. A. (2024). Unveiling the tapestry: A comparative investigation into data-protection legislation in India and Pakistan. *SOCRATES*, 1(28), 1–8. <https://doi.org/10.25143/socr.28.2024.1.01-08>
- Big Brother Watch and Others v. the United Kingdom, Apps. Nos. 58170/13, 62322/14 and 24960/15 (Eur. Ct. H.R. 2021).
- Bridges, R (on the application of) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058.
- Bunnings Group Limited and Privacy Commissioner [2026] ARTA 130.
- Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982.
- Clearview AI Inc. v. British Columbia (Information and Privacy Commissioner), 2026 BCCA 67.
- Commissioner Initiated Investigation into Kmart Australia Limited (Privacy) [2025] AICmr 155.
- Data (Use and Access) Act 2025, c. 18 (UK).
- Data Protection Act 2018, c. 12 (UK).
- Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
- Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (India).
- European Convention on Human Rights, Nov. 4, 1950, 213 U.N.T.S. 221.
- Glukhin v. Russia, App. No. 11519/20 (Eur. Ct. H.R. 2023).
- Human Rights Act 1998, c. 42 (UK).
- Human Rights Committee. (1988). General comment No. 16: Article 17 (Right to privacy).
- Human Rights Committee. (2024). Concluding observations on the second periodic report of Pakistan (CCPR/C/PAK/CO/2).
- International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
- Investigatory Powers Act 2016, c. 25 (UK).
- K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Matar, R., & Murray, D. (2025). Re-thinking international human rights law's approach to identity in light of surveillance and AI. *Human Rights Law Review*, 25(3), ngaf016. <https://doi.org/10.1093/hrlr/ngaf016>
- Office of the Australian Information Commissioner. (2026, July 29). Privacy Commissioner publishes updated guidance on facial recognition in retail spaces.
- Office of the United Nations High Commissioner for Human Rights. (2025). The right to privacy in the digital age (A/HRC/60/45).
- Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).
- Personal Data Protection Bill, 2023 (Pakistan) [draft/private member's bill; not enacted].
- Prevention of Electronic Crimes Act, 2016 (Pakistan), as amended by the Prevention of Electronic Crimes (Amendment) Act, 2025.
- Privacy Act 1988 (Cth) (Austl.).
- Privacy and Other Legislation Amendment Act 2024 (Cth) (Austl.).
- Privacy Act, R.S.C. 1985, c. P-21 (Can.).
- Rana, A., & Iqbal, A. (2025). Privacy and surveillance: Legal and technical perspectives. *UCP Journal of Law & Legal Education*, 3(2). <https://doi.org/10.24312/ucp-jlle.03.02.552>
- United Nations General Assembly. (2024, December 17). The right to privacy in the digital age (A/RES/79/175).
- United Kingdom Government. (2025). Police use of facial recognition: Factsheet.

- ◆ **Funding**
This research received no external funding
- ◆ **Conflict of Interest**
The authors declare that they have no known financial or personal conflicts of interest that could have influenced the work reported in this paper.
- ◆ **Data Availability Statement**
All data used in this study are derived from publicly available legal sources, including statutes, judicial decisions, treaties and published academic literature cited in the references. No new datasets were generated or analysed.
- ◆ **Ethical Statement**
Ethical approval was not required because this study is based exclusively on publicly available legal documents, judicial decisions, treaties and published literature, and did not involve human participants, animals or confidential data.
- ◆ **AI Use Disclosure**
Generative artificial intelligence tools were used in a limited and assistive capacity during the preparation of this manuscript, primarily for idea development, language refinement, and grammatical correction. The authors retain full responsibility for the originality, accuracy, analysis, interpretation, and final content of the manuscript.

JOURNAL POLICIESJuriSocial Journal of International Law

OPEN ACCESS & LICENCE All articles are freely available on publication under CC BY-NC 4.0. Readers may share and adapt the work for non-commercial purposes with proper attribution.	COPYRIGHT Authors retain copyright and grant JJIL the right of first publication.
PEER REVIEW Every research article undergoes double-blind peer review by at least two independent reviewers.	PUBLICATION ETHICS JJIL follows the Committee on Publication Ethics (COPE) Core Practices and guidelines.
PLAGIARISM POLICY All submissions are screened with similarity-detection software; plagiarism in any form leads to rejection.	GENERATIVE AI POLICY AI tools cannot be listed as authors. Any substantive use must be disclosed; authors remain fully responsible for the content.
CORRECTIONS & RETRACTIONS Errors are corrected through published corrigenda; retractions follow COPE guidelines.	ARCHIVING & INDEXING Content is preserved through [PKP Preservation Network / LOCKSS]. DOIs are registered with Crossref.
PUBLICATION CHARGES No article publishing fee charged	DISCLAIMER The views expressed are those of the authors and do not necessarily reflect the views of the editors or the publisher.

Submissions & enquiries editor@jjil.jurisocial.org