RIGHT TO PRIVACY, SURVEILLANCE AND DATA PROTECTION

R. Jacob, VELS School of Law, Pallavaram

Dr. Ashwathi Sukumaran, Professor, VELS School of Law, Pallavaram

ABSTRACT

The digital age has reshaped the relationship between individuals and the state, and privacy has felt the strain. This article examines the legal and constitutional dimensions of privacy rights, state surveillance powers, and data protection frameworks. By tracing how privacy jurisprudence has evolved, examining statutory surveillance mechanisms, and assessing contemporary data protection legislation, it argues that meaningful privacy protection needs clear legal standards, strong procedural safeguards, and independent oversight. Drawing on constitutional principles, judicial precedents, and comparative legal analysis, it shows how legal systems try to strike a balance between individual privacy rights and legitimate state interests in national security, public order, and crime prevention. The point is plain: even though the right to privacy is now widely recognized as fundamental effective protection still depends on the specificity of legal provisions, judicial oversight, and redress mechanisms.

CHAPTER-1

Introduction

Digital technologies have sprinted ahead, and they've reshaped modern life, making everyday routines more convenient, efficient, and connected across almost every corner of human activity. But there's a catch. That same shift has brought fresh risks for personal data. Once information lives in electronic form, and once surveillance tools get sharp enough, privacy becomes much easier for both state and non-state actors to poke into, steal, or misuse. This tension between privacy and security isn't new, but it feels sharper now, with mass data collection, algorithmic surveillance, and data moving across borders all the time. Governments around the world say they need broader surveillance powers to deal with terrorism, serious crime, and new threats to public order. People, meanwhile, want more control over their personal information and protection from arbitrary state intrusion. So the legal problem is plain: how do you protect legitimate state interests without hollowing out privacy, which sits at the heart of human dignity and democratic governance? First, it traces privacy's constitutional and human rights roots, from an implied safeguard to an expressly recognized fundamental right in many jurisdictions. Second, it turns to state surveillance powers across different legal frameworks, weighing the reasons governments give for those powers against the safeguards needed to keep abuse in check. Third, it looks at modern data protection legislation as the institutional piece that makes privacy rights real in the digital ecosystem. The analysis pays particular attention to recent developments in India, where the Supreme Court's landmark decision in Justice K.S. Puttaswamy v. Union of India (2017)[1] declared privacy a fundamental right, followed by the enactment of the Digital Personal Data Protection Act, 2023.

CHAPTER-2

Constitutional Roots of Privacy

Privacy's recognition as a fundamental right marks a real turning point in constitutional law across democratic societies. Unlike speech or religion, which constitutions often say outright, privacy usually enters the picture through judicial interpretation linked to bigger ideas of liberty, dignity, and autonomy. In India, that shift hit especially hard. For years, earlier

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India), ¶ 1-22.

Supreme Court rulings seemed to suggest the Constitution didn't protect a general right to privacy at all. In M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1963)[2], the Court held that privacy did not fall within the fundamental rights in Part III of the Constitution. That view rested on a narrower reading of constitutional protection, one that stuck to express text rather than implied rights. Then came the the Puttaswamy judgment of August 24, 2017, when a nine-judge bench of the Supreme Court delivered a unanimous, historic decision. The Court set aside its earlier precedents and held that the right to privacy is a fundamental right protected under Articles 14 (equality), 19 (freedom of speech and expression), and 21 (right to life and personal liberty) of the Constitution. The Puttaswamy decision takes privacy in a wide, almost layered way, across three distinct dimensions. Bodily privacy comes first, and it shields the physical body from unauthorized intrusion, including medical interventions, searches, and forensic procedures. Decisional privacy comes next; it protects personal choices about marriage, sexuality, family, and the other intimate stuff of life. Informational privacy, for its part, gives individuals control over the collection, use, and dissemination of their personal data. Put together this three-part framework shows that privacy works on several levels, from physical integrity to personal autonomy to data self-determination. The Court also made plain that the right to privacy, like all fundamental rights, isn't absolute. The state can limit it only if three conditions line up: the restriction must be authorized by law, it must serve a legitimate state aim, and it must be proportionate to the objective sought to be achieved. This approach leans heavily on the American constitutional idea of "compelling state interest." The Court adopted strict scrutiny, so any measure that cuts into privacy has to stay tightly drawn and do exactly what it claims. If a law overreaches and leaves the state room to pry into privacy beyond what's strictly needed for a specific threat, it won't pass constitutional scrutiny. The proportionality test works on several levels. First, there has to be a valid law, not just an executive directive or an administrative guideline. Second, the purpose has to be legitimate, usually national security, public order, crime prevention, or protecting the rights of others. Third, the means chosen must have a rational link to the objective. Courts have to look past a bare legal basis for privacy infringement and check the procedural safeguards, the specificity of the grounds invoked, and whether oversight mechanisms are actually in place.

[2] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India); M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).

CHAPTER-3

State Surveillance: Legal Frameworks and Constitutional Challenges

States have long claimed the power to intercept communications and collect information for national security and law enforcement. In India, that authority rests on several statutes, especially the Indian Telegraph Act, 1885, and the Information Technology Act, 2000. Section 5(2) of the Telegraph Act lets the government intercept messages "on the occurrence of any public emergency" or in the "interest of public safety." Here's the thing: the provision has drawn heavy criticism for vagueness, because neither "public emergency" nor "public safety" has a clear definition, which leaves plenty of room for executive discretion. Section 69 of the Information Technology Act takes a similar line, authorizing the government to intercept, monitor, and decrypt information sent through computer resources on grounds such as the sovereignty and integrity of India, national security, public order, or the prevention of crime. Those provisions came under challenge in People's Union for Civil Liberties[3] v. Union of India (1997), where the Supreme Court dealt with the issue head-on. The Court said surveillance can serve legitimate state goals, but only if it comes with real procedural safeguards. It required interception orders to come from designated authorities, to run for specific periods, and to face periodic review so misuse doesn't slip through the cracks. That's the basic check on the power. Still, surveillance law keeps bumping into overbreadth, where provisions give the state authority to gather far more information than any legitimate purpose needs. And that creates two dangers: arbitrary enforcement against disfavored individuals or groups, and function creep, where data collected for one thing gets reused for something else entirely. I think that second risk is easy to miss, but it's a big piece of the puzzle. In In Shreya Singhal v. Union of India (2015), a free speech case at heart, the Court drew privacy-relevant lessons when it struck down Section 66A of the Information Technology Act. The Court said laws that curb fundamental rights have to stay tightly drawn, with clear dfeinitions and predictable application. So when surveillance laws miss that mark, handing out sweeping discretion without real limits, they sit on shaky constitutional ground. Overbreadth hurts most in mass surveillance programs. They collect communications and metadata from entire populations, not just specific suspects. By design, they go well beyond what's needed to investigate a particular threat, scooping up huge amounts of information about people under no suspicion at all. That lack of particularization, the idea that surveillance should target

[3] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India), ¶ 23-28.

specific individuals for specific reasons, cuts against the constitutional rule that privacy intrusions must be proportionate and narrowly tailored. I think that point matters a lot. Still, substance isn't the whole story. The constitutional validity of surveillance laws also depends on the procedures that govern how they operate. In Puttaswamy, the Court made clear that procedural safeguards are what make a restriction "fair, just, and reasonable" under Article 21. I've seen this again and again: without those safeguards, the whole setup starts to wobble. The key procedural safeguards have a few parts. Prior judicial authorization means a surveillance order gets the green light from an independent judicial officer, not just executive authorities, so necessity and proportionality get an impartial look. Writing and recording requirements are simpler: the grounds for surveillance have to go down in writing, leaving a record that can be checked later. Time limits stop the the order from running on forever, so it needs periodic renewal. Destruction requirements force the deletion of information gathered through surveillance once interception has served its purpose. Independent review mechanisms add outside oversight bodies with power to audit surveillance activity and order the destruction of unlawfully obtained information. Without these safeguards, the constitutional picture changes fast. If the law offers no independent oversight, no written justification, and no post-surveillance review, the risk of arbitrary privacy invasion jumps sharply. I think that's the real issue here. Such regimes fail the proportionality standard because they lack

CHAPTER-4

Data protection laws as the institutional fix

Traditional privacy law relied on ex post remedies, like damages for intrusion upon seclusion, public disclosure of private facts, or misappropriation of likeness. Those tort claims still matter, but they're getting too blunt for the mess of systematic, large-scale data collection and processing. By the time someone learns their data has been misused, the harm may already be wide-ranging and hard to roll back. That's the turning point. It has pushed the move toward regulatory data protection frameworks. Unlike tort law, which depends on individual lawsuits, data protectoin legislation sets ex ante rules for data collection, processing, and transfer. Data fiduciaries (controllers) have to meet notice, consent, security, and purpose limitation obligations whether or not any individual has suffered a concrete harm, and regulatory authorities can audit, issue directives, and impose sanctions for violations.

Big picture, this approach starts from a simple fact: informational privacy can't rest on individual enforcement alone. The gap in information and resources between data subjects and data processors, plus the collective action problems baked into privacy protection, makes structural, institution-level mechanisms necessary. India's Digital Personal Data Protection Act (DPDPA)[4], enacted in August 2023 after years of legislative back-and-forth, is the country's first big data protection law. It lays out the rules for collecting, storing, and processing personal data by private entities and the state. The DPDPA also brings in a few key ideas. Data fiduciaries, the entities that decide the purpose and means of data processing, have duties around notice, consent, purpose limitation, data quality, and security. Data principals, the individuals whose personal data gets processed, have rights to access, correction, erasure, and grievance redress. the Data Protection Board of India serves as the regulator, with power to investigate violations and impose financial penalties. For cross-border transfers, the Act takes a "blacklist" approach, allowing transfers to That's a major step back from earlier legislative drafts, which had required data localization, and it reflects industry worries about how restrictive transfer rules would affect day-to-day operations. The DPDPA also creates significant data fiduciaries, entities that handle huge volumes of data, high-risk data, or work in politically sensitive sectors. They face extra obligations: data protection impact assessments, independent audits, and the appointment of data protection officers. Still, the hottest flashpoint in the the DPDPA is its carve-outs for state processing, especially in Section 36. That provision gives the government broad power to make data fiduciaries and intermediaries turn over any information it wants, on grounds like the "interest of sovereignty and integrity of India," "security of the State," or "performance of any function under any law." Critics argue that Section 36, along with the corresponding rules, repeats the same old problem. The grounds are vague and sweeping, and they leave executive discretion without the limits it needs. There's no requirement for prior judicial authorization, no notice to affected individuals that their data has been disclosed, and no independent review of whether the government's demand is lawful. That gap with surveillance rules in other Indian statutes really matters. The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009, require interception orders to come only from designated authorities, to be written down, and to be reviewed every two months by a review committee that can order destruction of information collected beyond the order's scope. Section 36 of the DPDPA doesn't even meet that basic floor. I think

[4] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 2-33

that's the real issue. It sets up a constitutional tension, because the Puttaswamy[5] framework says privacy limits need procedural safeguards. A provision that that lets the state collect personal data without judicial oversight, written reasons, time limits, or post hoc review is a problem.

CHAPTER-5 CONCLUSION

The right to privacy has moved out of the shadows of constitutional text and taken its place as a fundamental right, one tied to human dignity and personal autonomy. The Puttaswamy decision marked real turning point. It set out a framework that tries to balance privacy with legitimate state interests through legality, necessity, proportionality, and procedural safeguards. Still, the gap between constitutional principle and statutory reality remains wide. Surveillance laws keep giving state agencies broad, loosely defined powers, and too often they leave out the judicial oversight, transparency, and redress mechanisms the constitutional framework calls for. Data protection legislation is a major step forward, but it still carries exemptions that could easily repeat the failings of earlier laws. Closing that gap takes sustained effort from all three branches of government. Courts need to keep a close eye on surveillance laws and data processing practices, and they must demand compliance with constitutional standards. Legislatures need to tighten weak provisions and put in the procedural safeguards that make privacy limits fair, just, and reasonable. Executive authorities need to use surveillance powers sparingly, because the legitimacy of state action depends on respect for fundamental rights. The privacy-security tension isn't a zero-sum game. Societies can be safe and free at the same time, secure and still respectful of individual dignity. The trick isn't choosing one value over another; it's building institutions and legal rules that hold them together, protecting privacy as a fundamental right while still recognizing legitimate state interests.

[5] Puttaswamy, supra note 2, at ¶ 235-240 (Chandrachud, J., concurring) (enumerating procedural safeguards).

REFERENCES

1. NLS Forum, "Privacy, Surveillance, and State Interest: Appraising the DPDP Act through a Constitutional Perspective" (2025)

2. IAPP "Top 10 operational impacts of India's DPDPA – Cross-border data transfers" (2025)

3. Nigerian Journals Online, "Navigating the Tensions Between Data Privacy and National Security" (2025)

4. ScienceDirect, "Enhancing IoT privacy with artificial intelligence" (2025)

5. universitas Jember, "Intelligence Surveillance, Counterterrorism, and the Right to Privacy in Indonesia and Canada" (2025)

6. Taylor & Francis, "Balancing Privacy, Security, and and Civil Liberties" (2025)

7. EBC Webstore, "Right to Prviacy in India: From Judgment to Law" (2025)

8. IJLMH, "Privacy in Technology Innovation and The Challenges it Creates for Implementing the GDPR and India's DPDP Act" (2025)