INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE PANOPTIC SORT: RECONSTRUCTING THE RIGHT TO PRIVACY IN THE AGE OF ALGORITHMIC SURVEILLANCE

AUTHOR – DR PAULINE PRIYA S, PRINCIPAL AT ST JOSEPHS COLLEGE OF LAW, BENGALURU

BEST CITATION – DR PAULINE PRIYA S, THE PANOPTIC SORT: RECONSTRUCTING THE RIGHT TO PRIVACY IN THE AGE OF ALGORITHMIC SURVEILLANCE, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (1) OF 2026, PG.1053-1057, APIS – 3920 – 0001 & ISSN – 2583-2344. DOI https://doi.org/10.65393/WHPC1647

ABSTRACT

The right to privacy, once conceived as the fundamental right to be let alone, faces an existential crisis in the digital age. The pervasive extraction, analysis, and commodification of personal data by state and corporate actors have transformed privacy from a question of secrecy to one of power and autonomy. This article undertakes a socio-legal analysis of this transformation, examining how jurisprudence is evolving often belatedly to address challenges posed by surveillance capitalism, algorithmic decision-making, and the dissolution of public/private boundaries. It argues that traditional individualistic frameworks are inadequate to protect collective social identities and autonomy. By analyzing landmark case law from 2024 and 2025 across multiple jurisdictions including the Supreme Court of Canada's rulings, the Supreme People's Court of China's data rights cases, and significant American jury verdicts this paper charts the emergence of new legal theories. It explores concepts of privacy as trust, group rights to privacy, and statutory torts as mechanisms to recalibrate the balance of power. The article concludes that safeguarding privacy in the contemporary moment requires a paradigm shift: moving from protecting individual secrets to regulating the technological and commercial infrastructures that enable mass surveillance, thereby preserving the conditions necessary for democratic participation and individual autonomy.

Keywords: Right to Privacy, Digital Age, Surveillance Capitalism, Algorithmic Governance, Data Protection, Socio-Legal Studies, Autonomy

I. Introduction: The Dissolution of the Private Sphere

The historical conception of privacy, famously articulated by Warren and Brandeis as the "right to be let alone," was built upon a clear demarcation between the private individual and the public sphere. This model presumed that privacy was invaded through direct intrusion—a trespass upon property, the publication of a private letter, or the uninvited photographic gaze. In the 21st century, this architecture of separation has collapsed. The digital age is defined not by intrusion, but by extraction. Every search query, geolocation ping, social media interaction, and consumer transaction generates a data point that is harvested, analyzed, and fed into algorithmic systems designed to predict and influence behavior.[2380]

This transformation, termed "surveillance capitalism" by Shoshana Zuboff, repurposes human experience into behavioral data that functions as a commodity.[2381] The consequence is a fundamental power shift: personal information is no longer merely a reflection of identity but a raw material for corporate and state control. As Vejandla notes in a recent

[2380] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

[2381] Hemanth Vejandla, The Shifting Role of Privacy: Insights into Digital Governance, Societal Trust, and the Commodification of Autonomy in the 21st Century (2025) (Macquarie University Research Data Repository).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

thesis, privacy in the twenty-first century is "deeply entangled with corporate surveillance, algorithmic decision-making, and state control," reshaping the balance of power by turning personal data into a "negotiable commodity."[2382]

The law, a comparatively conservative institution, has struggled to keep pace. Traditional legal frameworks, predicated on individual harm and binary concepts of secrecy, are ill-suited to address the systemic and often invisible nature of digital surveillance. However, a wave of recent jurisprudence and legislative reform signals a growing judicial and societal awareness of the stakes. Courts are being asked to determine if an IP address deserves constitutional protection,[2383] whether tech giants can be held liable for deceptive data collection,[2384] and how to define the very nature of a search in a world where our communications are mediated by third-party platforms. This article analyzes these developments, arguing that they represent a slow but crucial move toward a more robust, socially-aware conception of privacy.

II. The Inadequacy of Individualistic Privacy Models

The dominant legal paradigm treats privacy as an individual right—a form of property or a zone of personal autonomy. This model falters in the face of Big Data, which derives its power from aggregation and inference.

A. The Limits of Consent

The primary mechanism for legitimizing data collection in the commercial sphere is "notice and consent." Users are presented with lengthy, often incomprehensible privacy policies and must click "I agree" to access a service. This ritualistic consent is a fiction. It places an impossible cognitive burden on individuals while offering no meaningful choice. As legal scholar Anuj Puri argues, a century old individualistic conception of privacy is "incapable of protecting her autonomy and identity when she is being targeted on the basis her interdependent social and algorithmic group affiliations."[2385]

B. From Individual Secrecy to Social Trust

Ari Waldman offers a compelling alternative, reconceptualizing privacy not as an individual right against the world, but as a matter of "trust" embedded in social relationships.[2386] He posits that disclosures occur in contexts of trust, defined by experience, shared identity, and relationships. When an individual shares information with a doctor, a bank, or a social media platform, they do so within a context that implies an obligation of confidentiality and appropriate use. The violation of privacy, therefore, is a betrayal of that trust. Waldman argues that privacy law "should be used to protect relationships of trust, rather than to protect a collection of individual rights."[2387] This framework better captures the harm when a platform like Facebook shares user data with a political consulting firm like Cambridge Analytica the harm is not merely the loss of secrecy, but the betrayal of the trust users placed in the platform.[2388]

Case Law in Flux: Charting a Right to Digital Privacy

The theoretical evolution of privacy is being mirrored, albeit unevenly, in courtrooms across the globe. Recent decisions reveal a judicial willingness to extend traditional protections to new technological contexts, though significant fragmentation remains.

A. Canada: Protecting the "Digital Breadcrumbs"

The Supreme Court of Canada has been at the forefront of adapting constitutional privacy protections to the digital age. The Court

[2382] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019).
[2383] R v Bykovets, 2024 SCC 6 (Can.).
[2384] Rodriguez v. Google LLC, No. 3:20-cv-04688 (N.D. Cal. 2025).
[2385] Anuj Puri, A Theory of Privacy, Cornell J. L. & Pub. Pol'y ,2020
[2386] Ari Ezra Waldman, Privacy as Trust: Sharing Personal Information in the Twenty-First Century, 69 U. Miami L. Rev. 559 (2015).
[2387] Ibid
[2388] Australian Information Comm'r v. Meta Platforms Inc., (proceedings discontinued 2024) (discussed in King & Wood Mallesons, *New avenues, new exposures: The evolution of privacy class actions, (Oct. 17, 2025)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

[2389]addressed the question of whether an individual has a reasonable expectation of privacy in their IP address. In a 5-4 decision, the majority ruled that they do. Writing for the Court, Justice Karakatsanis recognized that an IP address is the first "digital breadcrumb" that can lead police to a person's entire online life. The Court adopted a "normative approach," focusing not on what the police were looking for in that specific instance, but on what the IP address *could* reveal about a person. These ruling mandates that police obtain prior judicial authorization to request an IP address from a third party, extending Charter protection to a key piece of digital identifying information.

This logic was further refined in a subsequent matter [2390], which dealt with police viewing and responding to text messages on a locked phone's screen. While the Court was fragmented, the plurality affirmed that individuals retain a reasonable expectation of privacy in the substantive information contained in text message conversations, even if the initial "ping" is visible. These cases demonstrate a sophisticated understanding that privacy inheres not just in the content of communications but in the aggregate of information that digital trails reveal.

B. United States: Common Law and Statutory Torts in Action

In the United States, where a comprehensive federal privacy law is absent, plaintiffs have increasingly turned to state constitutional provisions, common law torts, and class actions. The 2025 jury verdict the federal jury in California awarded $425.7 million in compensatory damages to a class of approximately 98 million users. The plaintiffs successfully argued that Google continued to collect data even after users had disabled the "Web & App Activity" setting. The jury found this to be an invasion of privacy under California's constitution and a common law intrusion upon seclusion, even without a finding that Google collected personally identifiable information.[2391]

This verdict is significant for several reasons. First, it shows that juries are willing to hold tech companies accountable for deceptive design choices, or "dark patterns." Second, it establishes that the harm from data collection is cognizable even when the data is "anonymized" and used in aggregate. The jury's award, while far less than the $31 billion sought, signalled that the act of unauthorized collection itself constitutes a compensable injury. Google has announced its intention to appeal, arguing the jury misunderstood its privacy too.

C. China: Judicial Guidance in a State-Led Digital Economy

Even in jurisdictions with different political traditions, the judiciary is engaging with data rights. In August 2025, the Supreme People's Court of China released its first set of landmark cases concerning data rights protection. [2392]The Court noted a "noticeable increase" in data-related cases, with the number concluded in 2024 being double that of 2021.[2393] The released cases cover unfair competition and personal information protection, specifically addressing disputes arising from the collection of personal information by mobile apps. The SPC's goal is to "unify judicial standards" and create a "sound rule-of-law environment," highlighting that even in a state-centric model, legal frameworks are needed to manage the tensions inherent in mass data collection.[2394]

IV. Legislative Responses and the Rise of Group Privacy

The inadequacy of purely judicial remedies has spurred legislative action, with lawmakers attempting to create clearer causes of action and stronger penalties.

[2389] Supra note 4
[2390] R v Campbell, 2024 SCC 42.
[2391] Supra note 5
[2392] Ari Ezra Waldman, Privacy as Trust: Sharing Personal Information in the Twenty-First Century, 69 U. Miami L. Rev. 559 (2015).
[2393] Ibid
[2394] Australian Information Comm'r v. Meta Platforms Inc., (proceedings discontinued 2024) (discussed in King & Wood Mallesons, New avenues, new exposures: The evolution of privacy class actions (Oct. 17, 2025)).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A. Australia's Statutory Tort and the Class Action Landscape

Australia's Privacy and Other Legislation Amendment Act 2024[2395], which came into effect in June 2025, represents a significant legislative intervention. It introduces two key reforms: a direct statutory tort for serious invasions of privacy, and a new provision allowing courts to award compensation to individuals in civil penalty proceedings brought by the Information Commissioner.

The new tort requires a plaintiff to prove a serious invasion of that was intentional or reckless, and where there was a reasonable expectation of privacy. While proof of actual damage is not required, the threshold of "seriousness" may limit its application. The Australian law reflects a global trend toward creating specific, statutory remedies for privacy violations, moving beyond the "roundabout" causes of action like breach of confidence or negligence that plaintiffs previously had to rely on.[2396]

B. Theorizing the Collective: Group Rights to Privacy

These legal developments point toward a theoretical shift: the recognition that privacy is not merely an individual concern but a collective one. Puri's "triumvirate model of group right to privacy" is a sophisticated articulation of this. He argues that Big Data Analytics targets individuals based on their "interdependent social and algorithmic group affiliations." This "panoptic sorting" creates epistemic bubbles and distorts an individual's worldview through hyper-targeted content.[2397]

Puri's model posits three levels of group privacy:

1. Protects an individual's interest in their social identity, which is formed through participation in social groups.

2. Protects an individual's right to "informational self-determination" and against being unaccountably grouped by algorithms.

3. Recognizes that an organized group itself (e.g., a political association) may be entitled to privacy.

This framework is vital because it captures the harm of algorithmic profiling that never results in a specific data "breach." The harm is the systemic categorization and manipulation of populations based on inferred traits. Puri concludes, "our privacy is not only interdependent in nature, it is existentially cumulatively interlinked. It increases in force with each successive protection

V. Conclusion: Privacy as a Collective Necessity

The socio-legal battle over privacy in the digital age is, at its core, a battle over the distribution of power and the very conditions of autonomy. The traditional model, focused on individual secrecy and consent, has proven to be a paper tiger, easily shredded by the complex architectures of surveillance capitalism and state monitoring. The data points to a systemic issue: data breaches are rising, corporate surveillance is the default business model, and the legal system is only beginning to grasp the scale of the transformation.[2398]

The cases and statutes in the US, and the new Australian tort represent the leading edge of a necessary jurisprudential evolution. They show courts and legislatures starting to look beyond the immediate intrusion and consider the broader systemic effects. The Canadian Court's focus on the "digital breadcrumb" trail, the American jury's rejection of deceptive consent designs, and the Chinese Court's effort to standardize data dispute adjudication all point toward a more nuanced, context-aware understanding of privacy.

However, these are just the first steps. To fully address the challenge, the law must embrace

[2395] Privacy and Other Legislation Amendment Act 2024 (Cth) sch 2, s 80UA (Austl.).
[2396] King & Wood Mallesons, New avenues, new exposures: The evolution of privacy class actions (Jan 17, 2026).
[2397] Supra note 6
[2398] Supra note 9

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

the theoretical insights of scholars like Waldman and Puri. We must move toward a conception of privacy as *trust*, where the collectors and processors of data are held to the fiduciary standards implied by their relationships with users. We must also recognize the collective dimension—that our privacy is interlinked, and that the profiling of groups is an injury to every member of that group and to the democratic public sphere itself.

The right to privacy must be reconstructed. It is no longer sufficient to ask, "Is this information secret?" We must ask, "Is this flow of information just? Does it respect the trust of the individual? Does it allow for the free development of identity and the formation of a public sphere free from undetectable manipulation?" Privacy, in the digital age, is not just a personal right to be let alone; it is a collective necessity for a free society. Without a fundamental shift in how we frame and protect it, the promise of individual autonomy and democratic participation will continue to erode, traded away one click at a time for the convenience of "free" digital services.