The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ERASING THE DIGITAL PAST: A COMPARATIVE ANALYSIS OF THE RIGHT TO BE FORGOTTEN IN INDIA, THE UNITED STATES, AND THE UNITED KINGDOM

~ RAY PRIYA

ABSTRACT

Whether an individual may compel the removal of digitally preserved information about their past is among the most contested questions in contemporary information law. This article examines how India, the United States, and the United Kingdom have approached that question through constitutional text, primary legislation, and judicial decision and what their respective answers reveal about the deeper conflict between personal privacy and the public interest in an unimpeded flow of information. India's Digital Personal Data Protection Act, 2023 represents the country's first legislative attempt to translate the constitutional right to privacy, recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India, into an enforceable right of erasure. Against the backdrop of a First Amendment tradition that treats most restraints on truthful speech with deep suspicion, and a post-Brexit United Kingdom that has domesticated the European erasure framework but now charts an uncertain course of divergence, the article assesses the DPDPA's strengths, its structural omissions, and the unresolved tensions it leaves for adjudication. The central argument is that no jurisdiction has yet produced a satisfactory resolution of the privacy-expression conflict, and that principled adjudication requires a proportionality framework that gives real weight to both interests rather than treating either as categorically superior.

Keywords: Right to Be Forgotten; Digital Personal Data Protection Act, 2023; Informational privacy; Freedom of Speech and Expression; Comparative Data Protection Law.

I. INTRODUCTION

Before the internet became the dominant archive of public life, time performed a function that law rarely needed to replicate. Newspapers went out of circulation, court records sat in poorly indexed filing rooms, and embarrassing or damaging episodes from a person's past became practically inaccessible without deliberate archival effort. Search engines have dismantled that arrangement entirely. A conviction from three decades ago, a civil dispute resolved in a person's favour, an impulsive social media post from adolescence each survives in indexed, retrievable form for as long as the hosting server remains operational.[1] Law has been slow to catch up, and the right to be forgotten represents one of the most consequential attempts to do so.

As a doctrinal matter, the right to be forgotten refers to a data subject's entitlement to require a controller or processor to delete personal information that is no longer necessary for the purpose for which it was collected, or whose continued retention cannot be justified against the subject's interest in informational self-determination. The concept achieved its clearest early expression in European Union law, when the Court of Justice of the European Union held in Google Spain SL v. Agencia Española de Protección de Datos that ansasa individual could require a search engine to de-index links connecting their name to a newspaper article about a debt resolution proceeding that had long since concluded.[2] Article 17 of the General Data Protection Regulation later placed this principle on a firm statutory footing.[3]

India entered this space with the Digital Personal Data Protection Act, 2023,[4] which confers a statutory right of erasure under Section 12. The Act rests constitutionally on the ruling of a nine-judge bench of the Supreme Court in Puttaswamy,[5] where the Court held that Article 21 of the Constitution of India, guaranteeing the right to life and personal liberty,[6] encompasses an individual's right to control information generated about them. Yet the same Constitution, in Article 19(1)(a)[7] protects freedom of speech and expression a right that often stands in direct

[1]Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age 1–15 (2009).
[2]Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317, ¶ 99 (Ct. of Justice of the E.U. 2014).
[3]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 17, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[4]Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDPA].
[5]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[6]INDIA CONST. art. 21.
[7]INDIA CONST. art. 19(1)(a).

opposition to erasure claims, particularly when the information at issue concerns matters of public interest or historical record.

The United States presents a system where constitutional protection for expression has historically dominated. Without a federal omnibus privacy statute and with a First Amendment[8] that the Supreme Court has interpreted to forbid most government-imposed suppression of truthful information, American law has produced no general right to be forgotten. The United Kingdom, which retained a domesticated version of the EU framework after Brexit through the Data Protection Act 2018,[9] occupies a middle position that is substantively closer to the European model while institutionally and politically distinct from it.

II. INDIA: CONSTITUTIONAL FOUNDATIONS AND THE DPDPA FRAMEWORK

A. FROM ARTICLE 21 TO INFORMATIONAL PRIVACY

India's path to a statutory right of erasure runs through the jurisprudence of Article 21. Privacy does not appear in the text of that provision, which speaks simply of the right to life and personal liberty, but the Supreme Court in Puttaswamy ended a long period of doctrinal ambiguity by confirming that privacy is an intrinsic feature of human dignity that Article 21 protects. Crucially, the plurality did not confine this protection to physical privacy or decisional autonomy it extended it to informational privacy the entitlement of individuals to determine what data about themselves may be generated, retained, and shared.[10]

Before the DPDPA, courts responded to erasure claims by improvisation. The Madras High Court entertained petitions from individuals whose criminal acquittals or completed sentences were still visible on searchable judicial databases, reasoning that continued publication of this information served no legitimate public purpose once the legal proceedings had concluded.[11] However, these decisions lacked a coherent statutory framework. Judges reached for Article 21, occasionally supplemented by the law of breach of confidence or, in extreme cases, contempt of court, but the resulting remedies were inconsistent and difficult to enforce against online platforms domiciled outside India.

---

[8]U.S. CONST. amend. I.
[9]Data Protection Act 2018, c. 12 (UK) [hereinafter DPA 2018].
[10]Puttaswamy, supra note 3, at ¶ 119 (Chandrachud, J., concurring).
[11]Karthick Theodre v. Registrar General, High Court of Madras, W.P. (MD) No. 12015/2016 (Madras H.C. 2016).

B. THE DPDPA, 2023: ARCHITECTURE OF THE RIGHT TO ERASURE

Section 12 of the DPDPA confers upon every data principal the right to seek erasure of personal data held by a data fiduciary, subject to exceptions that are discussed below.[12] The right is triggered either by the withdrawal of consent or by the passage of the purpose for which processing was originally authorised.[13] This consent-centric structure reflects a deliberate legislative choice: rather than adopting an interest-balancing test at the point of erasure itself, the Act links the right to the pre-existing terms on which data was collected.

Broader provisions reinforce this architecture. Section 4 of the DPDPA requires that personal data be processed only on the basis of consent or for a specified legitimate use enumerated in the statute.[14] Sections 8 and 9 impose duties of accuracy and storage limitation on data fiduciaries, requiring them to delete or anonymise data once its stated purpose has been served. Taken together, these provisions embed a purpose-limitation principle that closely mirrors Article 5(1)(e) of the EU GDPR, though critics have rightly observed that the broad carve-outs available to state instrumentalities under Section 17 substantially weaken the regime as applied to governmental data processing.

Section 12(3) enumerates the circumstances in which a data fiduciary may decline an erasure request.[15] These include the performance of a statutory function, the fulfilment of a legal obligation, journalistic or research purposes, and the exercise of freedom of speech and expression. By naming expression as a ground for resisting erasure, the Act acknowledges the tension at the heart of this article but it leaves the actual balancing of competing interests to delegated rules and eventual adjudication, without providing the Data Protection Board with any statutory criteria for resolving the conflict.

C. THE CONSTITUTIONAL EQUILIBRIUM BETWEEN PRIVACY AND EXPRESSION

Article 21 and Article 19(1)(a) are both fundamental rights, and neither occupies a position of categorical priority over the other in Indian constitutional law. Article 19(2) permits reasonable restrictions on freedom of speech and expression on specified grounds,[16] and the Court has

[12]DPDPA, supra note 1, §§ 12–13.
[13]DPDPA, supra note 1, § 12(2)(a).
[14]DPDPA, supra note 1, § 4; id. §§ 8–9 (imposing obligations of data accuracy and minimisation on data fiduciaries).
[15]DPDPA, supra note 1, § 12(3)(a)–(e).
[16]INDIA CONST. art. 19(2).

consistently treated the protection of individual reputation and privacy as capable of justifying such restrictions when they are proportionate to the harm addressed. Equally, the Court in Puttaswamy acknowledged that privacy is not absolute and must yield when a sufficiently weighty countervailing interest is at stake.

Rajagopal v. State of Tamil Nadu, decided more than two decades before the DPDPA, established that the press may freely report upon the discharge of public functions by officials and public figures, but may not without consent publish information about their genuinely private affairs.[17] This public/private distinction, drawn from the Court's reading of American defamation law alongside Indian constitutional values, provides the interpretive grammar that courts and the Data Protection Board will need to apply when adjudicating whether an erasure request concerns information that legitimately belongs in the public record.

The institutional question may prove more difficult than the doctrinal one. The DPDPA establishes a Data Protection Board of India[18] as the primary adjudicatory body for erasure disputes. Unlike the European supervisory authorities and the UK's Information Commissioner's Office, both of which operate with statutory independence from government direction, the Board's composition and appointment procedure under the DPDPA vest substantial control in the executive. Whether a body so constituted can robustly adjudicate cases in which a state instrumentality is the respondent or in which disclosure of information embarrasses government is a question that goes to the structural integrity of the right rather than its textual scope.

III. THE UNITED STATES: FIRST AMENDMENT PRIMACY AND THE ABSENT FEDERAL RIGHT

A. THE CONSTITUTIONAL FRAMEWORK

American data privacy law must be understood against the backdrop of a constitutional provision the First Amendment that imposes severe constraints on government regulation of speech, including speech that others find harmful to their privacy, reputation, or dignity. Unlike the Indian constitutional scheme, which treats free expression and privacy as rights of equivalent constitutional status that must be mutually accommodated, American doctrine

[17]Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (India).
[18]DPDPA, supra note 1, §§ 33–40 (establishing the Data Protection Board of India and prescribing its powers and procedures).

begins from the presumption that content based restrictions on speech are unconstitutional. A right to be forgotten, in its fullest form, is essentially a content-based restriction it silences specific true information at the behest of the person to whom it refers.

Federal statutory privacy law is sectoral and patchy. The Privacy Act of 1974 creates rights of access and amendment against federal agencies but imposes no obligations on private entities.[19] The Children's Online Privacy Protection Act and the California Consumer Privacy Act address specific populations and business types, but neither establishes a general right to compel erasure of truthful information from search indices or third-party archives.[20] No federal statute analogous to Article 17 of the GDPR or Section 12 of the DPDPA exists, and repeated congressional attempts to enact one have stalled largely because of disagreement over its compatibility with First Amendment principles.

The foundational constraint was articulated in New York Times Co. v. Sullivan, where the Supreme Court held that robust protection for public discourse requires tolerance of statements that might, in a stricter regime, generate liability.[21] Although Sullivan concerned defamatory falsehoods about public officials, its underlying logic that liability rules which chill speech impose systemic costs on democratic discourse extends to the truthful statements that erasure regimes typically target. Courts and scholars have consistently read Sullivan as erecting a near-absolute barrier against compelled suppression of accurate information that is a matter of public record or public concern.

B. PRIVACY TORTS AND THEIR LIMITS IN THE DIGITAL CONTEXT

American common law has recognised a cause of action for the public disclosure of private facts since at least Melvin v. Reid, where a California court held that a woman who had lived as a reformed private citizen retained a protectable interest against having her former identity as a prostitute exposed in a commercially released film.[22] The Restatement (Second) of Torts codifies this tort but subjects it to a newsworthiness defence, and courts applying that defence in subsequent decades have given it an expansive reading that immunises most disclosures concerning matters of any plausible public interest.

[19]Privacy Act of 1974, 5 U.S.C. § 552a (2018).
[20]Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018) [hereinafter COPPA]; California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2022) [hereinafter CCPA].
[21]New York Times Co. v. Sullivan, 376 U.S. 254 (1964).
[22]Melvin v. Reid, 112 Cal. App. 285 (1931).

Garcia v. Google, Inc. illustrates the difficulty of achieving erasure through non-privacy theories. The claimant sought removal of a film from online distribution, but the Ninth Circuit ultimately resolved the case on copyright grounds, expressly declining to develop a freestanding privacy right to compel content removal.[23] This pattern of litigants using copyright, defamation, and harassment law as proxies for privacy relief that American law does not directly provide produces unpredictable outcomes tied to the doctrinal accident of which adjacent cause of action can be stretched to fit the facts. The transaction costs are high, the outcomes uneven, and the remedy unavailable to those whose situations do not happen to fall within an adjacent tort.

Pavesich v. New England Life Insurance Co. demonstrated that American courts were capable, at the turn of the twentieth century, of recognising a free-standing right to privacy grounded in natural law and personal autonomy.[24] That early trajectory was eventually overtaken as media law developed in the shadow of the First Amendment. Whether a resurgent interest in data rights evident in state-level legislation and renewed academic and legislative debate will produce a meaningful federal privacy framework remains an open question, but the First Amendment constraint is structural, not merely political, and any federal erasure right would need to be designed with that constraint in view.

C. STATE-LEVEL RESPONSES

In the absence of federal action, state legislatures have moved at different speeds and in different directions. California's Consumer Privacy Act, which took effect in 2020, confers a right to deletion of personal information held by covered businesses, subject to exceptions for public interest, freedom of expression, compliance with legal obligations, and certain research purposes.[25] Other states have adopted comparable legislation, but the lack of uniformity means that a data subject's ability to obtain erasure depends heavily on state of residence, the operational location of the data controller, and the specific category of data. Crucially, no state statute has convincingly resolved how a deletion right applies to search engine indexing the context in which the practical need for erasure is most acute.

IV. THE UNITED KINGDOM: POST-BREXIT HYBRIDITY AND THE PROPORTIONALITY MODEL

[23]Garcia v. Google, Inc., 786 F.3d 733 (9th Cir. 2015) (en banc).
[24]Pavesich v. New England Life Insurance Co., 122 Ga. 190 (1905).
[25]California Consumer Privacy Act, supra note 20, § 1798.105(d)(1).

A. THE STATUTORY FRAMEWORK AFTER BREXIT

Brexit created a need for the United Kingdom to establish a domestic legal basis for data protection obligations that had previously been satisfied through direct application of EU law. Parliament addressed this through the Data Protection Act 2018 and through the retention of a domesticated and amended version of the GDPR, now referred to as the UK GDPR.[26] Article 17 of the UK GDPR mirrors the erasure right conferred by its EU counterpart, entitling data subjects to require erasure where personal data is no longer necessary for its original purpose, where consent has been withdrawn without any other lawful basis for processing, or where the data has been processed unlawfully.

The Information Commissioner's Office serves as the principal supervisory authority under the DPA 2018 and UK GDPR.[27] In contrast to India's Data Protection Board, the ICO operates with statutory independence and has over two decades of accumulated expertise in data protection adjudication. Its guidance on the right to erasure, though not legally binding, is regularly cited by tribunals and courts, and it structures the practical compliance behaviour of data controllers and processors across all sectors.

B. NT1 & NT2 V. GOOGLE LLC: PROPORTIONALITY AT WORK

No English judgment has addressed the right to be forgotten with greater care than NT1 & NT2 v. Google LLC[28] decided by Mr Justice Warby in the Queen's Bench Division. The two claimants identified only by these pseudonyms both sought de-indexing of Google search results that linked their names to news coverage of criminal convictions. NT1 had been convicted in the 1990s for a business-related conspiracy offence and had served a custodial sentence; NT2's conviction, for a tax-related offence, was spent under the Rehabilitation of Offenders Act 1974. The contrast between their situations allowed the court to apply a detailed and revealing proportionality analysis.

NT1's claim failed. The court found that his offending was directly connected to the conduct of his commercial affairs, that he had never publicly acknowledged the conviction or expressed remorse, and that there remained a legitimate public interest in the accurate reporting of

[26]DPA 2018, supra note 26; UK General Data Protection Regulation, art. 17 [hereinafter UK GDPR] (retained EU law as modified by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, SI 2019/419).

[27]Information Commissioner's Office, Right to Erasure, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-uk-gdpr/individual-rights/right-to-erasure/ (last visited May 10, 2026).

[28]NT1 & NT2 v. Google LLC [2018] EWHC 799 (QB) (Eng.).

conduct by persons in positions of commercial responsibility.[29] NT2's claim succeeded. His conviction was legally spent, he had genuinely reformed, his offending bore little connection to his current professional activities, and there was no continuing purpose served by the search results that was proportionate to the ongoing injury to his reputation and private life.

The court's methodology drew directly on the factors identified in Google Spain[30] the nature and sensitivity of the data, the claimant's role in public life, the passage of time, the accuracy of the information and the legitimate interest of the public in retaining access. This analysis was conducted through the lens of the Human Rights Act 1998, which incorporates Articles 8 and 10 of the European Convention on Human Rights into domestic law[31] requiring courts to balance the right to private life against the right to freedom of expression. NT1 & NT2 demonstrates that a proportionality based approach, applied by an appropriately equipped and independent judicial or quasi-judicial body can produce outcomes that are principled and individually sensitive.

C. JURISDICTIONAL LIMITS AND POST-BREXIT DIVERGENCE

Two sets of concerns shadow the UK framework going forward. The first is territorial. In Google LLC v. CNIL,[32] the Court of Justice of the EU confirmed that de-indexing obligations under the GDPR do not extend to non-EU versions of a search engine's service. The UK's analogous framework raises identical questions: a person who secures an erasure order against the UK version of a search engine may find their information accessible through the search engine's versions in other jurisdictions. Neither the DPA 2018 nor any court order has definitively resolved the extraterritorial reach of UK erasure obligations meaning that practical erasure may be incomplete even where legal entitlement is established.[33]

The second concern is legislative drift. Since Brexit, the UK government has expressed interest in reforming the UK GDPR to reduce compliance burdens on businesses, and the right to erasure has been identified in reform consultations as an area warranting review. Any significant weakening of the erasure right risks triggering a reassessment of the UK's adequacy status under the EU GDPR without which cross-border data flows between the UK and EU

[29]NT1 & NT2, supra note 29, at ¶ 87.
[30]Google Spain, supra note 6, at ¶ 99.
[31]Human Rights Act 1998, c. 42, sch. 1, pt. I, arts. 8, 10 (incorporating the European Convention on Human Rights into domestic law).
[32]Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL), Case C-507/17, ECLI:EU:C:2019:772 (Ct. of Justice of the E.U. 2019).
[33]European Convention on Human Rights arts. 8, 10, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

member states would require alternative legal safeguards. This tension between domestic regulatory preference and international data trade dependencies has no obvious resolution, and its outcome will substantially determine the practical scope of the erasure right for UK residents.

V. CONCLUSION

The right to be forgotten is not a demand to falsify history. It is a claim that the permanent, effortless retrievability of personal information imposes costs on individuals particularly on those who have reformed, who were wrongly implicated, or whose past disclosures were made in circumstances that no longer obtain that cannot always be justified by a genuine and continuing public benefit. That claim deserves to be taken seriously, and the legal systems examined in this article have, to varying degrees, begun to do so.

None of them has yet done it well. The United States, constrained by a constitutional tradition that privileges expression with unusual intensity, has produced no general right and leaves most individuals without remedy against truthful disclosures that nonetheless cause ongoing harm. India has provided a right whose scope and enforcement remain uncertain, whose institutional guardian lacks structural independence, and whose exceptions are drafted at a level of generality that invites inconsistency. The United Kingdom has the most developed jurisprudence and the most credible regulatory institution, but faces structural challenges about territorial scope and political pressure to weaken protections in the name of economic flexibility.