

The Right to be Forgotten and Judicial Activism

Kushagri

LL.M

University Institute of Legal Studies, Chandigarh University.

Abstract:

This study looks at how courts have influenced the creation, application, and enforcement of the "Right to be Forgotten" (RTBF) in three legal orders: the US, the EU, and India. Courts have done this through judicial activism or restraint. The study tracks institutional processes, significant court rulings, legislation frameworks, and doctrinal advances that impact the harmony between freedom of expression and privacy. It contends that the most robust and enforceable RTBF regime has been produced by the EU's data-protection framework and jurisprudence; India has an emerging, case-driven RTBF that has been greatly influenced by activist courts and piecemeal rulings; and the US opposes an RTBF analog due to First Amendment protections and decentralized regulatory structures.

Keywords: RTBF, Data Protection, Decentralized, Laws.

INTRODUCTION

Personal information is now much more persistent and accessible because to digital technologies. Content that was once lost over time can now be found and shared at any time. The right to request the removal or delisting of personal data from search results or repositories, also known as RTBF, addresses the negative effects of an enduring digital record, including intrusion, reputational harm, and the chilling of private life. However, the RTBF lies at the nexus of conflicting constitutional and human rights values: freedom of expression, public interest, and historical record on the one hand, and privacy and personal dignity on the other. In order to clarify how judicial behavior influences RTBF outcomes in practice, this comparative analysis places important court rulings and legislative frameworks in three jurisdictions: the US, India, and the EU.

Under RTBF, judicial activism assumes a particularly important role. Even in the absence of comprehensive law, courts can adopt an inclusive approach by developing remedies that safeguard dignity and privacy. Judicial restraint, on the other hand, limits the role of courts in establishing standards for digital privacy by emphasizing deference to lawmakers. The interpretation, application, and enforcement of the RTBF are directly impacted by the judicial philosophy that each jurisdiction has chosen.

The RTBF sits at the nexus of societal interests and fundamental rights. On the one hand, it gives people back control over their digital identities while safeguarding their privacy, autonomy, and sense of dignity. However, it also touches on issues of freedom of expression, public interest, and historical transparency. It is difficult to strike a balance between these conflicting ideals since it frequently entails arbitrary assessments of whether information is "relevant," "accurate," or "necessary" for the general public to know. As a result, courts are essential in establishing and upholding the RTBF, especially in areas where legislative frameworks are lacking or changing.

With an emphasis on India, the European Union (EU), and the US, this article compares and contrasts the RTBF. The EU exemplifies a developed, institutionalized RTBF policy with its historic Google Spain ruling and subsequent implementation in the General Data Protection Regulation (GDPR). In particular, after the Supreme Court recognized the right to privacy in *K.S. Puttaswamy v. Union of India* (2017),

India exhibits an emergent RTBF that has been significantly influenced by judicial interventions. Due to strong First Amendment protections, the US offers few RTBF-like remedies and instead relies on market-based solutions and sector-specific laws. Through an analysis of these jurisdictions, the study demonstrates how legislative frameworks, constitutional principles, and judicial behavior all work together to establish the boundaries of digital privacy rights in the contemporary day.

I. LEGAL AND INSTITUTIONAL FRAMEWORK

• European Union – Statute and Judicial Doctrine

The General Data Protection Regulation (GDPR) and CJEU case law serve as the foundation for the EU's current RTBF architecture. The Court of Justice of the EU (CJEU) concluded in the landmark case of *Google Spain v. AEPD and Mario Costeja González* (C-131/12) that search engines process personal data and must comply with requests to remove links when the data is "inadequate, irrelevant, or no longer relevant." This court decision balanced privacy interests against public-interest factors, establishing a remedial responsibility on controllers (search engines). In addition to strengthening data-subject rights, administrative enforcement, and cross-border collaboration among data-protection agencies, the GDPR later codified a right of erasure (Article 17), institutionalizing channels for RTBF-style relief across Member States.

• India – Constitutional Posture and Law development

In contrast to the GDPR, India does not currently have a single, unified legislative RTBF in effect. But in *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court acknowledged privacy as a fundamental right, creating doctrinal room for RTBF arguments under Article 21 (life and personal liberty) and expressive-rights balancing under Articles 19 and 14. Through judicial pronouncements and interim orders, subsequent High Court decisions and tribunals have granted delisting/removal orders in specific contexts, such as cases involving survivors of sexual assault or where materials are erroneous, irrelevant, or unduly detrimental to dignity. This effectively creates RTBF remedies. Indian courts have occasionally ordered removal from private intermediaries or archives based on the principles of informational privacy and dignity.

• United States – Constitutional Constraints and Fragmented Regulation

The US has minimal federal statutory protection comparable to the EU's GDPR and no acknowledged constitutional RTBF. One significant limitation of the First Amendment is that courts frequently examine content-removal policies for possible speech suppression. Scholarly research and court rulings indicate that the US is unlikely to enact a comprehensive RTBF on par with that of Europe because strong free-speech safeguards frequently clash with forcing search engines or publishers to take down legally published content. The FTC and state privacy laws, such as California's CCPA/CPRA, have delegated regulatory authority over platforms in the US, resulting in a patchwork system that may address specific privacy concerns but does not establish a general erase right. Different public-interest weightings and constitutional obstacles stand in the way of attempts to incorporate RTBF concepts into the US.

II. JUDICIAL ACTIVISM: DEFINITIONS, MODES, AND RELEVANCE TO RTBF

• What is Judicial Activism

In order to achieve justice or public interest objectives, courts may interpret constitutional or statutory provisions broadly, filling legislative gaps, developing remedies, or aggressively enforcing rights. This approach is known as judicial activism. Decisions where judges seem to go too far by essentially creating policy are frequently referred to as "activist" by critics. Judicial activism in the context of RTBF can take the form of courts enforcing responsibilities on intermediaries, recognizing privacy rights in the absence of explicit legal mandates, or directing the removal of content to preserve autonomy and dignity. In contrast, judicial restraint narrowly interprets rights to maintain democratic lawmaking and yields to legislative solutions.

The Significance of Judicial Activism for RTBF

Because it necessitates striking a balance between privacy and public record and expression, RTBF is fundamentally policy-laden. Through active interventions, courts can offer prompt, case-specific remedies in situations where legislators are sluggish to act or offer insufficient protection, as is the case in India and historically in the US. The RTBF was institutionalized in the EU through a regulatory environment (GDPR) that was successfully sparked by judicial activism (CJEU interpretation). Ad hoc RTBF remedies have been developed in India by activist courts. However, courts in the US have largely refrained from drafting RTBF regulations that would conflict with constitutional speech guarantees, illustrating how activism or restraint influences the emergence of an enforceable RTBF.

III. JURISPRUDENTIAL CASE STUDIES

1) EU: GOOGLE SPAIN (C-131/12) AND FOLLOW-ON RULINGS

The CJEU decided in Google Spain that the search engine is a data controller and may be forced to take down links to personal information when the interests of the data subject outweigh those of the public. Individual balance and determining whether the information is "inadequate, irrelevant, or excessive" were stressed by the Court. The reach of delisting and its extraterritorial bounds were modified by later jurisprudence, which included rulings on territorial scope (such as Google v. CNIL and similar cases). The EU approach creates structured processes for removal requests, appeals, and consequences for noncompliance by combining judicial interpretation with administrative enforcement through data-protection authorities and standardized legislative rights under the GDPR. This model exemplifies the Court's interpretive extension, or judicial activism, which sparked the development of administrative and legislative architecture.

2) India: K.S. Puttaswamy and Post-Puttaswamy RTBF Orders

Puttaswamy laid the doctrinal groundwork for RTBF claims in India by establishing informational privacy as a basic right. Following Puttaswamy, a number of High Courts have mandated the removal of internet content when its continued availability violates someone's dignity, privacy, or rehabilitation (e.g., libelous or outmoded records, rape victim name removals). Case-specific and fact-sensitive, Indian judicial interventions have occasionally ordered internet intermediaries or archives to remove items from their lists. These court decisions are a blatant example of activism motivated by the desire to protect rights, since they represent the de facto judicial construction of RTBF remedies due to incomplete statutory systems. However, detractors caution that until more precise legislative guidance or administrative procedures are put in place, there may be inconsistencies and possible overreach.

3) United States: First Amendment Limits and the Absence of a Judicially Created RTBF

Although US courts have considered privacy damages, they have been hesitant to accept a universal RTBF that would mandate the removal of accurate, legally published material. Any content-removal regime must meet strict standards set by constitutional free-speech rights; forced removal may be considered content suppression. There are tailored remedies (criminal statutes, tort law, and limited injunctions) for serious privacy breaches (such as doxxing and the sharing of explicit photographs without consent), but these are not equivalent to a comprehensive RTBF. Instead of being enforced by a judicially formed RTBF, the outcome is a disjointed, frequently market-driven approach to content filtering and privacy protection. The question of whether and how to create erase mechanisms that are compatible with the constitution is still up for dispute.

IV. COMPARATIVE ANALYSIS

Institutional Pathways to RTBF

EU: Strong, administratively mediated RTBF is the result of judicial interpretation (CJEU), a comprehensive statutory framework (GDPR), and empowered regulators. Google The institutionalization was sparked by Spain.

India: Supreme Court's constitutional recognition of privacy combined with fragmentary High Court rulings and litigation resulted in an emergent RTBF that was influenced by judicial activism but lacked a standardized statutory process. Doctrinally, Puttaswamy is crucial.

US: Limited, tailored protection with no overall RTBF due to First Amendment restrictions, sectoral/state regulations, and market/compliance processes.

Balancing test and standards

The EU employs an interest-balancing strategy that, as understood by data-protection principles, balances the public interest in access against privacy dignity. Without established protocols, India's courts have applied proportionality and dignity concerns in individual instances, frequently drawing inspiration from international standards. Broad RTBF remedies are more challenging to uphold in US courts, which often lay a greater burden on claimants to demonstrate a compelling state interest to support speech restrictions.

Enforcement and Extraterritoriality

Although territorial issues (such as delisting globally vs. geo-limited) spark continuous discussion and legal action, EU authorities and the GDPR offer tools for cross-border enforcement and collaboration. The practical reach of India's rulings is frequently restricted (removal from particular platforms or sites located in India), which makes it difficult to enforce against international platforms. Extraterritorial enforcement is irregular and reliant on agreements with platforms or specific laws because the US lacks a centralized regulator to regulate cross-border erasing.

Political and Cultural Drivers

Divergent cultural commitments to privacy and free expression underline these institutional differences. The EU historically prioritizes data protection as a core social value; India's emerging jurisprudence reflects constitutional dignity and rapid judicial engagement with rights; the US foregrounds open public discourse and legal protections for publishers, constraining RTBF-style remedies.

V. CONCLUSION

The Right to Be Forgotten sits at a critical nexus of digital memory, privacy, and dignity. Judicial activism is crucial in defining the parameters of RTBF in countries like India where statutory frameworks are new or disputed. However, such activism needs to be doctrine-bound, principled, and cohesive. A balanced RTBF framework must incorporate technical, procedural, and institutional safeguards, adopt a structured proportionality test, and balance public interest and individual remedy. Clarity in the statutes combined with careful but restrained judicial scrutiny is the best course of action.