Rohini Toal

Data Privacy Ruling:
Domestic Implications of the Supreme Court's Ruling and a Comparative Analysis

Every click, swipe, and search leaves a trace of the user, a digital footprint; and unlike footprints in sand, digital footprints never wash away. As societies digitise, personal data has become both a valuable commodity and a source of vulnerability.

Social media, as a valuable commodity, enables people to build large audiences, positively influence others, and even find gainful employment through digital platforms. This power to connect and amplify voices gives it immense social and economic worth. Yet this very openness also makes it deeply vulnerable: the same material can be exploited to create manipulative or harmful content.

Consider, for instance, the recent rise in deepfake scams: parents in India and abroad have been tricked into transferring money after receiving fabricated audio messages of their children crying for help, allegedly under arrest (Thakur, 2024). Similarly, images and voices scraped from social media have been repurposed into fake content or manipulated videos. (The Times of India, 2025; Mishra, 2024). Women, in particular, face disproportionate harm, with their images and voices being repurposed into fabricated or sexually exploitative content without consent (Pandey, 2025). In such cases, victims are often left uncertain whether their data has been fully removed after reporting abuse, or whether it continues to circulate unseen in digital archives and shadow platforms (Fortra, 2025).Part of the reason is that the removal process involves complex layers, such as archiving for legal compliance, algorithmic suppression, cryptographic erasure, or partial visibility restrictions. While cryptographic erasure offers a technical means to render data inaccessible without fully deleting it, its use is rarely disclosed (Fortra, 2025). This further blurs the line between deletion and concealment. This opacity leaves data principals uncertain about the finality of removal, raising concerns over both transparency of data fiduciaries, and trust in how their requests are handled.

This uncertainty is reflected in the sheer volume of formal requests made for data removal. Thus far, Google has received 4,32,403 requests for de-listing of URLs by data principals. These data principals are those individuals whose personal data is being collected, processed, and stored by the organisation, commonly known as a data fiduciary. Of the removal requests made by data principals, 62.4% were de-listed by the platform, the data fiduciary. (Google Transparency Report, 2025).

According to X, formally Twitter, India submits the fourth highest requests globally for legal takedown (X Transparency Center, 2022a; 2022b). The number of requests in 2024 averaged at 80,000 (Google Transparency Report, 2025). A number of factors can contribute to this surge, such as a rapid increase in number of digital users with the onset of the pandemic, increasing government scrutiny over online content, and the use of takedown requests as a tool to manage misinformation and politically sensitive material (Business Line, 2023). These numbers illustrate both a growing demand from citizens and governments to exercise control over their data, and the mounting pressure on intermediaries to respond in a transparent manner.

The management of politically sensitive material has been particularly contentious: during the 2021 farmers' protests in India, several accounts and tweets critical of government policy were withheld at official request (Perrigo, 2021). In Turkey, thousands of posts were ordered

removed after the 2016 coup attempt (Wong, 2016); and takedown requests from Russia includ content related to opposition figures and protests (Litvinova, 2021). These examples illustrate how takedowns often sit at the intersection of public order concerns and debates over freedom of speech.

The management of politically sensitive material has been especially contentious, as critics argue that takedown orders are often used to suppress dissent, satire, or unfavourable reporting, raising concerns about the erosion of freedom of speech and democratic accountability (Vengattil, Chaturvedi, & Kalra, 2025). Supporters, however, contend that such measures are necessary to curb hate speech, incitement, and destabilising misinformation, making the political debate around takedowns deeply polarised (Aryan, 2021).

In this realm of data permanence lies a dilemma of the 21st century: how much control should individuals have over their own data, and how far should governments go in protecting it?

The answers differ depending on which legal and cultural systems one looks at, reflecting not just regulatory choices, but deeper values about autonomy, speech, and sovereignty. This article attempts to answer this dilemma by laying out approaches various countries have adopted to address data privacy.

The Evolution of Data Protection

The foundations of modern data protection lie in Europe. France's *droit à l'oubli* ("right to oblivion") began as a criminal law tool allowing rehabilitated convicts to request a removal of their names from official records (Sharma, 2020). In the 1990s, Spanish businesses began arguing that outdated financial records online were causing reputational damage. The most famous case, *Mario Costeja González v. Google (2014),* pushed the EU's Court of Justice to declare search engines as "data controllers" with obligations under European law (Agarwal & Singh, 2025).

Thereafter, Europe consolidated its approach with the General Data Protection Regulation (GDPR) 2018, enshrining rights such as access, rectification, portability, and the Right to Be Forgotten (RTBF) under Article 17 (Agarwal & Singh, 2025). In India, the Supreme Court recognised RTBF under the Right to Privacy, as part of the fundamental rights' framework. Thus, while RTBF is a headline-grabber, it should be understood as part of a larger move towards strengthening privacy protections in law (The Hindu, 2025).

This legal trajectory shows how data protection has evolved from isolated disputes into a more structured regime. Let's take a closer look at how data privacy is addressed in different cultural and legal contexts.

India: Rights-Based Approach

As governments across the globe race to define how far protections should go, their starting points could not be more different. In India, this debate plays out against a vast digital divide, wherein only 24% of rural households have internet access, compared to 66% in the cities. (NIIT Foundation, 2024). Digital literacy therefore remains patchy, and the majority of the

data principals- general users- are unaware of how their personal data is collected, monetised, or retained.

To tide over this, the Supreme Court in *K.S. Puttaswamy v. Union of India (2017)* recognised privacy as a fundamental right (The Hindu, 2025). This is grounded in Helen Nissenbaum's *Contextual Integrity Theory*, wherein privacy is violated when information leaves the context in which it was originally shared (Agarwal & Singh, 2025). The Digital Personal Data Protection Act, 2023 (DPDP) operationalises this by defining rights for data principals, and duties for data fiduciaries. It also creates a limited right to erasure, often described as India's step towards RTBF (Ministry of Law and Justice, 2023).

Additionally, the Reserve Bank of India's (RBI) data localisation mandate, or *Data Diktat*, requires payment platforms and intermediaries to store and process consumer information within domestic boundaries (Money Control, 2024), a trend that could soon extend beyond financial services.

Denmark: Copyright as Protection

Denmark has chosen an integration between government and markets, leaning towards copyright-style regulation, especially in the context of deepfakes and identity theft. Here, a person's likeness, face, or voice is treated as their intellectual property. Unauthorised replication would therefore be considered a violation, similar to copyright infringement. Under this model, if a person reports a deepfake, platforms are legally obliged to remove it, or they face significant fines. This approach finds its base in Alan Westin's "privacy as control" idea, but through property law instead of human rights (Agarwal & Singh, 2025).

Advantages of this approach include faster enforcement, clearer obligations, and direct platform liability, rather than requiring individuals to pursue lengthy legal action. Exceptions are built in for satire and parody, but otherwise the law prioritises quick removal and deterrence. This model is more market responsive, signalling to platforms that enforcement costs will be high, unless they are proactive in investing in monitoring and compliance systems.

Comparative Understanding

While India's approach addresses data privacy and deepfakes as part of a broader privacy agenda, ensuring citizens' rights are realised; Denmark's framework sets predefined penalties and takedown obligations for quicker results.
India embeds deepfake protection inside a constitutional rights framework; Denmark treats it as a property rights issue, applying established copyright-like protections.

The European Union's (EU) new AI Act 2024 introduces yet another dimension to this landscape. By regulating high-risk AI systems, including those generating deepfakes or processing sensitive personal data, the Act moves beyond individual rights or property frameworks to focus on systemic accountability (AI Act, 2025). This signals a shift towards anticipatory regulation, ensuring that risks are mitigated before they scale.

This contrast highlights a broader truth: rights-based systems preserve dignity but risk delay, while property-based systems deliver speed but may overlook non-economic harms. In

practice, hybrid systems, wherein rights would be constitutionally guaranteed and platforms face clear liability, may prove the most effective balance.

Challenges in Regulating and Ensuring Data Privacy

While governments face the challenge of conceptual ambiguity in balancing privacy with freedom of expression and public accountability, there is also a difficulty in defining what constitutes information pertaining to public interest. Clearer guidelines can therefore mitigate this ambiguity.

Platforms on the other hand, face operational hurdles in applying diverse national standards across jurisdictions, especially when cross-border data flows are common. Harmonised regional or bilateral agreements could reduce these frictions, while preserving local regulatory autonomy.

Citizens face the challenge of navigating regulatory hurdles, especially given the nature of cross-border data flows, and the absence of standardised measures. The average data principal often lacks the awareness to make meaningful requests, leading to under-enforcement of rights. Public education campaigns, assisted access mechanisms, and simplified complaint systems can address these gaps.

Another challenge is the asymmetrical power dynamics between large tech firms and individual users, where companies hold far greater capacity to delay or dilute compliance. Stronger penalties, independent oversight authorities, and collective international redressal mechanisms could rebalance this power. The Facebook 'shadow profile' controversy, where deleted data remained stored in invisible form, exemplifies this imbalance and underscores why enforcement must be both independent and transparent (Brandon, 2018).

Way Forward

Data privacy and deepfakes are not just individual problems, they are a societal challenge. They undermine trust in information, create new tools for harassment, and erode the credibility of both private citizens and public institutions. The experience of Denmark shows the importance of swift enforcement, while India's constitutional framing demonstrates the need for protecting the vulnerable populace. A blended approach could serve as a global best practice.

For India, the way forward lies in bridging the awareness gap among data principals, ensuring that fiduciaries are held accountable, possibly extending localisation mandates beyond payments to personal data. While the RBI's data localisation mandate initially targeted payments data, the principle is beginning to take shape beyond financial services. Increasingly, policymakers under India's IT Rules (2021) are considering whether Over-The-Top (OTT) platforms, social media intermediaries, and streaming services that process sensitive user information, should also bear obligations of storage and deletion within India's jurisdiction (PRS, 2021).

Global companies would need to keep a track of these increasing localisation mandates and adapt compliance systems accordingly.

As governments diverge, citizens must navigate uneven protections across borders. The future of data privacy will depend not just on laws or platforms, but on how societies choose to approach and navigate digital permanence.