International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Justice in the Age of the Internet: Balancing Transparency of the Judiciary and the Right to be Forgotten

Dr. Satyaprakash Swain

Principal, Bhubaneswar Law College, (Affiliated to Madhusudan Law University, Cuttack)

Abstract:
True justice involves not only a fair trial inside a courtroom, but a legal framework that prohibits persistent digital stigmatization outside of it. The traditional notion of judicial openness held that court proceedings and documents had to be open to the public, as a vital check against institutional abuse and to encourage responsibility. But the digital age has radically altered this dynamic. What once was secured by the "practical obscurity" of paper archives (the sheer physical friction of getting them) is now always searchable, discoverable, and indexable via a simple web search.
This paper explores the growing tension between the fundamental right to publicity in the courts and the nascent 'Right to be Forgotten'. It claims that the weaponization of open court records on the public internet creates a permanent digital banishment that significantly diminishes an individual's right to rehabilitation, personal privacy, and economic mobility long after their legal concerns have been put to rest. This essay advocates for a fair judicial standard by examining existing legal gaps and the conflict in global privacy frameworks. It proposes a tiered approach to public access, arguing that the basic operations of justice should be visible, but that the free digital distribution of personal identifiers needs to be constrained to protect human dignity and the opportunity for a fresh start.

Keywords: Right to Be Forgotten, Judicial Transparency, Digital Stigma, Public Records, Privacy Law, Freedom of Information.

I. Introduction:

The idea of real justice as a two-sided coin: a fair trial in the courts and the end of lasting digital stigma outside of it. The move from "practical obscurity" (physical friction of paper archives) to immediate, always-on digital availability.The conflict between public accountability (Judicial Transparency) and personal dignity/rehabilitation (Right to Be Forgotten). It is necessary to allow for review of court rulings to hold the judiciary accountable, but the unrestricted spread of personal identifiers on the web that may be indexed causes excessive damage. True justice requires a modern, tiered system that harmonizes open courts with the right to a digital clean slate.

II. The Rise of Judicial Transparency and the Death of "Practical Obscurity":

A. The Historical Foundations of Open Courts:

Public justice is a basic pillar of democracy . The democratic need for clear justice has always served as an ideological defence against institutional tyranny. The legal system, by requiring that courtroom doors remain open, set up a crucial check on governmental authority, preventing abuses that secret tribunals in the past generated, like the English Court of Star Chamber, and imposing rigorous judicial responsibility. Public scrutiny has a twofold role: it ensures a fair trial for the accused by putting witnesses and judges to the discipline of public observation, and it contributes to social trust in the integrity of judicial outcomes. The deeply ingrained common-law presumption of public access to court records arises from this necessity. This assumption means that judicial papers are not the private property of the litigants or the state, but public property open to examination. Under conventional common law theories, the public and the press have a qualified right to see and copy public records and documents, including judicial records... This access allows citizens to comprehend the law's operation, to see the performance of elected or appointed judiciaries, and to join in informed democratic discourse.

B. THE DOCTRINE OF "PRACTICAL OBSCURITY":

For centuries, the common law presumption of openness to the public coexisted with private privacy because of an unwritten, structural protection: the theory of "practical obscurity." This idea, famously expressed by the United States Supreme Court[1],where it acknowledges the substantial, legally meaningful gap between information available in public repositories and information gathered into a readily accessible digital profile.

In the age of paper archives, physical barriers naturally served to balance competing interests of public transparency and personal privacy. If a neighbour, employer, or journalist wanted to access an individual's court records, they had to work through high transactional friction. They had to physically drive to the courtroom where the matter was heard, ask a court clerk for the physical file during business hours, and pay per page for photocopies.

This logistical friction meant that when a trial was over and public interest waned, the documents simply fell into a state of benign neglect. This **"practical obscurity"** meant that the record was technically available to meet transparency standards but in practice unavailable to the casual browser. A person who had so cleared his legal problems had a practical clean slate, for his prior errors or legal conflicts did not automatically follow him into ordinary social and business dealings.

C. The Digital Revolution:

The emergence of the internet and digital court administration systems has torn away the protective veil of practical obscurity, ushering in a significant paradigm shift. Today, judiciaries around the world have moved to computerized file systems to boost administrative efficiency. But in the process they've unwittingly turned local court records into a consolidated data stream available globally.

This migration to digital has given rise to a predatory ecosystem of private third parties. Legal judgments are constantly being indexed by search engines and complex data brokers and private background check organizations use automated web scrapers to acquire, consolidate and commercialize judicial data. Criminal charges, family disputes, civil litigations that were formerly hidden away in basement filing cabinets are now geared for search engine algorithms. A simple Google search of someone's name can bring up an arrest record from ten years ago or a dismissed law suit noquestions asked.

The end effect is a modern "Scarlet Letter" that's permanent in digital form. Unlike the physical mark of old, this digital stigma is invisible but everywhere, attaching a person forever to his or her worst day or a legal battle long ago resolved. The internet never forgets, thus the public memory's usual temporal decay

[1] U.S. Department of Justice v. Reporters Committee for Freedom of the Press (1989).

has been erased, and individuals are constantly exposed to casual bias, social ostracization, and institutional hurdles to job and housing.

The core problem is that **the open courts doctrine** was intended to permit the public to watch the government and the judges, but in the digital age the public internet utilizes it to permanently watch and judge private individuals.

III. The Price of Permanent Memory: Digital Stigma and Human Dignity:

[This part moves the conversation from the structural change of the internet to the human, real-world cost of digital permanence.]

A. Socio-Economic Impact of Digital Banishment:

When judicial documents are pulled from their practical obscurity and posted on the public internet, they are no longer merely legal histories; they become vehicles of socio-economic exclusion. Today, risk-averse institutions increasingly evaluate persons with automated background checks and algorithms in the modern economy. Third-party background providers and data brokers often trawl court dockets and fail to update them with later dispositions. The digital record thus becomes an immutable, often false caricature of an individual's past.

The result of this automatic vetting is a type of digital exile from the modern market place. Empirical research repeatedly finds that even small or non-conviction information, such as arrests that did not lead to charges, dismissed civil actions, or evictions long ago, are total impediments to job, housing and financial credit.

[Public Record Scraped] ──> [Private Data Brokers] ──> [Automated Risk Assessment] ──> [Socio Economic Exclusion]

All too often, automated hiring algorithms or rental screening software reject an applicant before a human being even looks at the applicant's qualifications or hears the applicant's side of the story. This exclusion is damaging structurally: it excludes people from the formal economy, pushes them into insecure or under-the-table employment, and severely limits their spatial and social mobility.

B. The Psychological Effect of Continual Exposure:

Beyond the measurable economic damage, the constant availability of court data exacts a heavy psychological toll. The classical privacy theory maintains that the **"right to be let alone"** is a fundamental precondition for individual liberty and emotional health. The internet systematically erodes this right, it has no forgetting mechanism.

The possibility of a permanent digital record living in your shadow puts people in a constant state of hyper alert. The knowledge that any potential employer, new neighbour, landlord, or even a long-lost relative can find out their past in seconds with a simple web search results in chronic worry, embarrassment, and social isolation. This perpetual exposure blurs the boundaries between one's public and private self.

A person's most vulnerable or embarrassing moments—whether it is a bitter divorce custody fight, a bankruptcy record or a youthful misdemeanour—are permanently indexed alongside their professional profile. In this way they are essentially robbed of the ability to define their own identity in the present.

C. The Corruption of Legal Rehabilitation:

From a systems perspective, the persistence of digital stigma throws a deadly contradiction into the very idea of the justice system. Rehabilitation is a fundamental basis for systems of penal and civil law everywhere, the idea that someone who has broken a social or legal contract can be subjected to a penalty proportionate to that breach, reformed, and eventually accepted back as a fully integrated member of society.

Traditional Paradigm: [Offense] ──> [Proportional Penalty] ──> [Rehabilitation] ──> [Full Reintegration]

Contemporary Digital Reality [Offense] ──> [Proportional Punishment] ──> [Rehabilitation] ──>[Enduring Digital Stigma]

The weaponization of open court records directly undermines this cycle. By making a person's legal record always alive and viewable on the public internet, the digital ecosystem has extended their punishment forever. The law might say a sentence has been served, a debt has been paid, but the internet exacts a continuous, extra-legal toll. This undermines the State's goal in lowering recidivism and strengthening social cohesion. When the internet's infrastructure guarantees that a person's past will haunt them forever, the idea of legal rehabilitation is a cruel fantasy and a lifetime of digital disgrace replaces a journey of reform.

The existing system produces a deep paradox: the state puts large resources into rehabilitating individuals and helping them re-enter society, while simultaneously operating open-record systems that allow private data brokers to fully prohibit such re-entry.

Section IV: Comparative Law Landscape: Different World Frameworks
[**This section provides an overview of the technical and jurisdictional friction that occurs throughout the world. It discusses the diverse ways that judicial systems around the world address the privacy-transparency trade off]**]

IV. Divergent International Structures: Clashing Legal Frameworks:

The conflict between judicial transparency and the Right to Be Forgotten is not only an academic discussion; it has led to significantly different legal measures across the globe. The collision of digital and physical borders has produced two dominant legal traditions. The European tradition sees privacy as an extension of human dignity, whereas the Anglo-American tradition regards public transparency and free expression as almost absolute.

A. The European Model: GDPR and the Right to be Forgotten :

The European Union set the modern architectural plan for the Right to Be Forgotten. The idea was based on the historic **Court of Justice of the European Union (CJEU)** decision [2]. The **CJEU** found internet search engines to be data controllers. People have a right to ask search engines to remove links to websites holding personal information about them that is no longer relevant, accurate or of public interest.

This judicial precedent was finally enshrined into law as **the "Right to Erasure" in Article 17 of the General Data Protection Regulation (GDPR)**. Under the GDPR, data protection and human dignity are fundamental human rights, enshrined in the **EU Charter**. European jurisprudence directly provides this protection to judicial news and court registries.

The **GDPR** treads a narrow line here – data processing necessary for the exercise of the freedom of speech or to comply with a legal requirement is exempted – but increasingly, European judges are siding with the individual's right to move on. This is particularly true where the data subject is a private individual and a long time has elapsed since the judicial procedures came to an end. Further developments in the **CJEU** [3],

[2] Google Spain SL v. Agencia Espanola de Proteccion de Datos (2014).
[3] TU, RE v. Google (2022).

have reinforced this approach by requiring search engines to de-index results if an individual can show that the indexed judicial or commercial material is "manifestly inaccurate".

B. The Anglo-American Model: The First Amendment and Transparency First:

The Anglo-American legal tradition, led by the United States, has a strong presumption in favour of free speech and of the press, in contrast to the European concern for data privacy and human dignity. The U.S. First Amendment jurisprudence recognizes the essential right of the public to receive information about the government's operations, including the administration of justice.

The constitutional principle necessitating this course is that the State may not punish the dissemination of true material legitimately obtained from public court documents. The U.S. Supreme Court has consistently ruled that once court proceedings are open to the public, privacy rights must give way[4].

[European Model] Dignity/Privacy First —> Right to be forgotten (GDPR Article 17)
[Anglo-American Model] Transparency First —> First Amendment Absolute Protection

And the notion of a court-ordered "Right to Be Forgotten" is inconsistent with free speech in this context. Any attempt to force a private platform or search engine to withhold public court data is a highly questionable "prior restraint" on speech. Thus, the American legal system relies almost entirely on legislative back-end measures, such as formal expungement or sealing acts, that are completely separate from requiring internet intermediaries to clean up the public digital environment.

C. The Global Gap and the Jurisdictional Mess:

The clash of legal ideologies has generated a massive regulatory divide, creating jurisdictional turmoil beyond measure in the border less Internet. A web search query can traverse national boundaries in a flash, making it a logistical and legal nightmare to enforce localised privacy rights against global digital giants. In another decision[5] the CJEU curtailed the worldwide ambitions of the European model, bringing the friction to the fore. The court ruled that search engines must comply with de-indexing orders for all versions of their platform in the EU, but are not bound to de-reference globally across international domains (e.g., .com). To bridge that divide, search engines use geo-blocking to hide search results from users in a protected territory, while exposing them to the rest of the world.

The result is an unstable compromise produced by this geographic division. One can be successfully "forgotten" on European domains, but may be fully exposed on international platforms. And the fledgling common law judiciaries are increasingly involved in the crossfire.

D. Indian Scenario:

Here's the full elaboration on how budding common law judiciaries, especially honing in on the landmark 2026 verdict by the Delhi High Court[6], are handling this digital crossfire. A Detailed Discussion In common law countries such as India, where statutory regimes for data privacy are nascent or being established[7], the judiciary has had to step in to fill the legislative gap. This difficulty is acute: common law is traditionally predicated on the notion of stare decisis (precedent), and total openness of written, accessible records. But the computerized court records, by being continuously searchable by name, have in effect converted a prior legal disagreement into a life sentence extra-judicially. In the case of **Laksh**

4 Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975); The Florida Star v. B.J.F., 491 U.S. 524 (1989).
5 Google v. CNIL (2019)
6 Laksh Vir Singh Yadav v. Union of India (2026).
7 The Digital Personal Data Protection Act, 2023.

Vir Singh Yadav's[8] case, **Justice Sachin Datta,** in a landmark 144-page judgment on more than 35 consolidated writ petitions, has made the most comprehensive attempt of a common law court to manually carve out following sustainable middle ground **:-**

1. The Court resolved the tension between the right of the public to information and the right to privacy by immediately anchoring the **Right to Be Forgotten (RTBF)** within Article 21 of the Indian Constitution (the Right to Life and Personal Dignity). The Court, drawing from the basic privacy doctrine of **K.S. Puttaswamy v. Union of India**[9], held that informational privacy encompasses the ability of an individual to govern their public digital narrative and to safeguard their reputation from **"outdated truths".** Once a court action is over, the permanent public availability of an individual's personal identifiers under a name-based search can cause disproportionate harm that much exceeds any remaining public usefulness.
2. Operation of the **'Middle Ground'**:-The Delhi High Court, significantly, held that it could not set fire to the traditional house of open justice to save individual privacy. Hence, it devised a pragmatic two-pronged approach: **de-indexing and masking: De-Indexing** (The Search Filter): The Court has asked the commercial search engines (like Google) and the online legal repositories (like Indian Kanoon) to delist or disable the name-based searches in respect of certain judgments. With this process, the historical record itself is not erased from the digital cosmos. The case remains available to scholars, attorneys, and the public by citation number, legal provision or case name. But a simple search on the person's personal name will no longer lead to the stigmatizing legal record.
3. **Masking (The Redaction):** In cases of a very sensitive or private nature, the Court allowed for the redaction of names and personal identifiers within the digital text itself, using neutral labels (e.g. XYZ). For historical integrity, the full unredacted text of the ruling is retained in perpetuity in the court's internal archives. The **laksh vir singh yadav**[10] framework does not give carte blanche to rewrite history. The middle ground is a rigorous balancing criteria that outlines who is eligible for a digital clean slate, and who is completely barred: **Allowed for RTBF Relief :** Those who are totally acquitted, discharged ,closure or quashing, Parties in matrimonial disputes or family law proceedings, Litigants who are only mentioned in passing, Resolved commercial/civil matters• **Categorically Excluded for Relief:** Conviction for major offenses (particularly against women and children)• Cases involving public officials or a breach of public trust• Matters of legitimate and continuous public interest.

E. Scenario in Asia-Pacific and Eurasian countries:

Giving people control over their digital footprints is a global trend, which is reflected in the ideas I have highlighted above . Though official Right to Be Forgotten (RTBF) or "Right to Erasure" was made popular by Europe's GDPR, but Asia-Pacific and Eurasian countries have incorporated these ideas into their own legal systems, striking a balance between privacy, state authority, and business interests.

Expanding on Australia and Japan:

Japan: The Framework of APPI -

One of the earliest data privacy laws in Asia is Japan's Act on the Protection of Personal Information (APPI). People do not have a general "right to be forgotten" under the APPI just because they want

[8] Ibid.
[9] 2017 (10) SCC 1.
[10] Ibid.

something removed. Rather, there is a conditional right to request data suspension, deletion, or cessation of third-party provision.
It is activated if the data was obtained unlawfully, is being used without permission for purposes other than those specified, or if its ongoing use puts the person's rights or legitimate interests at risk of being violated.
Australia: The Changing Privacy Law -
The "Right to Be Forgotten" is not specifically codified in Australia's historic Privacy Act of 1988. However, if personal information is no longer required for any authorized purpose, Australian Privacy Principle[11] mandates that organizations take reasonable measures to "destroy or de-identify" it. The Current Situation: There are ongoing legislative proposals to establish a legal, explicit Right to Be Forgotten in order to offer Australians more direct control over deleting damaging or out-of-date internet information, following a thorough examination of the Privacy Act by the Attorney-General's Department.

The Situation in Russia and China:
China: PIPL (Personal Information Protection Law) -
The **Personal Information Protection Law** (PIPL) , which operates in tandem with the Cybersecurity Law and Data Security Law, greatly formalizes China's framework.
The Erasure Right: A right to erasure is clearly established by PIPL[12]. Under a number of circumstances, personal information processors 'must' remove data on their own initiative (or upon individual request):

1. The processing goal has been fulfilled, cannot be fulfilled, or is no longer required.
2. The product or is no longer offered by the company, or the storage time ends.
3. The person 'retracts their consent'.

The subtlety: Although Chinese residents have strong rights against private entities, these laws contain extensive carve-outs for national security and state organs, so requests for data deletion are typically not enforceable against state-run databases or government monitoring.

Russia: The"Delisting"Law for Search Engines -
By enacting a particular federal statute, Russia adopted a unique, highly tailored approach to the Right to Be Forgotten.
'Targeting Search Engines': Russian nationals have the legal right to request that search engines 'delist search results' linked to their names. Links may be deleted for the following reasons:
1. Handled against Russian legislation.
2. Clearly 'erroneous or false'.
3.Irrelevant or 'obsolete' as a result of later events (e.g., an old, insignificant historical episode that no longer carries public relevance).
The subtlety: Instead of requiring the host website to remove the underlying information, Russia's RTBF law primarily focuses on regulating what is viewable via public search engines, in contrast to the EU's GDPR, which broadly applies to data controllers.

[11].11.2 (APP 11).
[12] . Article 47

Current Situation in Other Asian Nations Country :|
Status of Right to Be Forgotten/Erasure :
India-The Digital Personal Data Protection Act (DPDP Act) grants citizens ("Data Principals") the explicit right to the correction, completion, and erasure of their personal data once the purpose for its collection is fulfilled or consent is withdrawn.
South Korea- Under the Personal Information Protection Act (PIPA), one of the strictest privacy laws in the world. The government has actively introduced guidelines for minors to remove their childhood digital footprints, and it has strong data deletion mandates when consent is revoked or the data lifecycle expires.
Singapore- The Personal Data Protection Act (PDPA) does not feature a broad Right to Be Forgotten. Rather, it emphasizes the "Right to Withdraw Consent." Organizations are required to cease collecting, using, or revealing data if a user withdraws consent, but they are not always required to remove historical backups if there is still a legitimate or commercial need.

F. The challenge of systems:

The **Laksh Vir Singh Yadav judgment**[13], a victory for human dignity, exposes the structural strain on common law judiciaries. The legislature has not created an automated, systematic method for deleting data, so courts must consider these petitions in a tedious case-by-case fashion. It compels the judiciary to play the role of a perpetual editor of the digital ecosystem – balancing the public's right to know under Article 19 against the individual's right to walk away under Article 21.

But, the international gap, without an international agreement, means people are at the mercy of their geography, as they must traverse a fractured digital reality where their past can be erased in one hemisphere, but remains forever broad casted in another. The current international deadlock is a structural flaw: the internet is borderless but the protection of data privacy is entirely territorial. This compels search engines to become quasi-judicial censors who decide where to draw the line between global free speech and local human dignity.

V: Closing the Gap: A Tiered Judicial Standard Proposal.

The current deadlock between judicial transparency and data privacy is rooted in a false binary worldview. Historically, the law has considered public records as an all-or-nothing affair: either a file is open to anybody or it is wholly sealed from view. In the analogue age, the friction of **"practical obscurity"** made this binary system work. But the digital age demands an impossible decision between total destruction of human privacy or eternal digital expulsion. To bridge this disparity this article suggests a modern legal framework: The Principle of Proportional Accessibility. Borrowing from the pragmatic mechanics of the Delhi High Court in **Laksh Vir Singh Yadav v. Union of India**[14] , this standard moves away from the question of whether a document should be public, and instead focuses on how and to whom such information should be accessible.

[Traditional System] —> Binary Choice —> [All-or-Nothing Exposure]
[Proposed System] —> Tiered Access —> [Accessibility Ratio]

A. The "Proportional Accessibility":

Principle Proportional accessibility recognizes that public interest in a court record is not static. That

[13] Ibid.
[14] Ibid.

interest diminishes over time and changes depending on the type of content. Legal scholars, journalists and practicing lawyers need unimpeded access to legal precedents and structural data to track the courts, but the general commercial internet has no legitimate civic interest in the long-term, name-based indexation of private persons. Judiciaries can be fully transparent about what the law is while limiting the easy weaponization of who was engaged by taking the legal substance of a judgment out of the personal identifiers of the litigants.

B. The Tiered Access System:

In order to apply this principle courts should adopt a uniform automated **Three-Tier Access Framework** for all judicial records kept in electronic form.

1. **1.Tier 1**: **Full Public Access (The Core Mechanisms):**For all legal concepts and institutional facts. All the structural elements of justice must be totally open, completely unredacted. It includes judicial reasoning, statutory interpretations, procedural rulings and the names of judges, prosecutors and public authorities. The documents must be completely searchable by citation, legal provision and keywords, to maintain historical continuity and public accountability.
2. **Tier 2: Conditional/Restricted Indexing (The Personal Identifiers):** Activated after acquittal, dismissal or lapse of time. The court has an obligatory de-indexing rule for private litigants, for non-serious offences and for a favourable conclusion (acquittal and discharge). Commercial search engines (e.g. Google, Bing) and private legal libraries are legally banned from indexing the case through personal name queries. The record remains available through conventional legal citation, but a casual search of a person's name will turn up no results and effectively return the individual to their practical obscurity.
3. **Tier 3: Automated Sealing & Personal Identifier Masking:**For extremely sensitive private litigations or small records.Family law, divorce conflicts, minor civil disputes or juvenile records have personal identifiers systematically concealed at source. The computerized judgment available to the public substitutes the names with neutral pseudonyms (e.g., XYZ v. State). The unredacted master copy is sealed and kept solely in the internal, secure archives of the judiciary, and is only available upon a showing of good legal reason before a court.

The Paradigm Fix: De-indexing Versus Deletion:

The conceptual win of this tiered standard is that it emphasizes de-indexing rather than the actual deletion or destruction of past files. That strikes at the crux of the fear among open-court traditionalists that the Right to Be Forgotten will lead to an Orwellian rewriting of legal history.

└──> **Internal Court Registry (Unchanged Historical Archive)**
[Public Court Case] ───┤ └──> **Commercial Web Search ── [DE-INDEXED by Name Searching]**

De-indexing, as the doctrine of **Laksh Vir Singh Yadav**[15]**,** does not change a word of the historical record in the court registry. For the purposes of legal research, appellate review and statistical analysis, the court archive is perfectly intact. Instead, de-indexing mainly impacts the public discoverability of such data on commercial, profit-oriented search platforms. It recognizes that a court record is a permanent fixture of legal history, but it should not be a permanent anchor around an individual's neck on the public internet. This tiered norm balances the institution’s transparency with the human right to a new digital life by

[15] Ibid.

regulating the commercial gateway to the data, not the data itself. The beauty of the tiered model is that it does not see privacy and transparency as mutually exclusive but as complementing. It keeps the precedent public, thus preserving the integrity of the law, and keeps the identity of the human being practically concealed, thereby preserving the dignity of the human being.

VI. Addressing Counterarguments and Implementation Challenges:

Any structural reimagining of public records inevitably invites intense scrutiny. Critics of the Right to Be Forgotten (RTBF) within judicial systems generally anchor their objections in three camps: constitutional protections for free speech, public safety considerations, and the sheer technical impracticality of regulating a borderless internet. Addressing these concerns is essential to demonstrating that a tiered judicial standard is not just theoretically noble, but legally and operationally viable.

A. The Freedom of Speech and Press Objection

The most potent constitutional objection—particularly within Anglo-American jurisprudence—is that restricting access to court records constitutes an impermissible infringement on freedom of expression and press freedom. First Amendment purists argue that the media and the public possess an absolute right to report on, discuss, and archive truthful information derived from public government operations. They contend that any judicial directive forcing a platform to suppress or delist a record amounts to an unconstitutional "prior restraint" or an attempt to forcibly edit public discourse.

However, this objection mischaracterizes the nature of a tiered accessibility framework. The proposed standard explicitly protects journalists' right to report on **live cases**. It places no restrictions on contemporaneous reporting, trial coverage, or investigative journalism while a matter is active or of immediate public concern.

[Live Trial / Active Case] ——————> Absolute First Amendment / Press Freedom to Report

[Post-Resolution / Decay Phase] ——> Tiered Access Applied Only to Name-Based Indexing

The restriction applies strictly retrospectively and narrowly to commercial, name-based search indexing after a case has concluded—particularly in instances of acquittals, dismissals, or minor offenses. Furthermore, because the framework targets search engine intermediaries and commercial data aggregators rather than the original journalistic source or the court file itself, the underlying speech remains entirely untouched. The article remains online; only the automated, casual, name-based gateway to it is modified.

B. The Public Safety Argument and the Multi-Factor Balancing Test

A second critical counterargument is rooted in public safety and the public's **"right to know."** Detractors argue that hiding or de-indexing certain judicial histories could inadvertently blind employers, financial institutions, or communities to real risks, such as hiring a fraudster or renting to a violent offender. They contend that public safety demands an immutable public memory to track recidivism and assess risk.

To prevent the Right to Be Forgotten from becoming a shield for ongoing public deception, the framework must eschew categorical absolutes. Instead, judiciaries should employ a standardized, **Multi-Factor Balancing Test** to determine eligibility for de-indexing or masking.

[INDIVIDUAL RIGHTS] [PUBLIC INTEREST]

Rehabilitation • Dignity • Expungement <—— BALANCE ——> Severity • Public Office • Recidivism Risk

When evaluating a petition for digital privacy, courts must weigh the following distinct metrics:

- **The Severity and Nature of the Offense:** Violent crimes, financial fraud targeting public funds, and sexual offenses are categorically barred from **RTBF** relief due to the permanent, compelling public safety interest in those records. Conversely, minor misdemeanours, civil contract disputes, and non-conviction data heavily favour the individual.
- **The Status of the Litigant:** Public servants, corporate executives accused of white-collar crimes, and prominent figures whose actions impact the public trust have a significantly reduced expectation of digital privacy. Private citizens thrown into the legal system by circumstance retain a robust claim to dignity.
- **The Element of Time and Recidivism Risk:** As the years pass since a case's disposition without further legal infractions, the public utility of the data decays exponentially, while the individual's right to rehabilitation increases.

By filtering petitions through this rigorous judicial screen, public safety is preserved, ensuring that the digital clean slate is an earned pathway toward rehabilitation rather than an avenue for fraud.

C. Technical and Administrative Hurdles: Regulating the Scraping Ecosystem

Even if the constitutional and philosophical arguments are satisfied, a daunting pragmatic question remains: how can a court effectively enforce a de-indexing order against a shadow ecosystem of private third-party data brokers and background check companies that have already scraped, cached, and stored the data offline? The internet is filled with jurisdictions that fall outside a local court's territory, and automated web scrapers copy court dockets within seconds of their publication.

While completely cleansing the internet is an impossibility, systemic administrative shifts can dramatically curb the harm:

1. **Algorithmic Gatekeeping (Robots.txt Protocols):** Courts must fundamentally redesign their electronic registries to prohibit commercial web crawlers from indexing personal identifiers. By encoding strict no-index commands into the metadata of court dockets, search engines like Google can be systematically blocked from mapping names to case files at the source, without affecting manual searches by authorized legal professionals.
2. **Enforcement via Statutory Liability:** Legislatures must back judicial de-indexing orders with strict statutory penalties for commercial data brokers. Under frameworks akin to the European GDPR or India's Act of 2023,[16] background check companies must face heavy financial liability if they fail to regularly sync their local databases with the court's updated, tiered registry. If a record is de-indexed or sealed by a court, the private broker must be legally mandated to scrub it within a specific window.

Ultimately, while the technical challenges are real, they are an argument for **better engineering and stricter regulation**, not for complete judicial surrender. The law has always adapted its enforcement mechanisms to match technological progress; managing the flow of digital court records is simply the next necessary phase of that evolution. The friction here is not actually between privacy and free speech, but between human rehabilitation and commercial data monetization. A tiered system respects journalists and protects the public, while drawing a hard line against data brokers who treat private human suffering as an open-source commodity.

VII. Concluding remarks:

Real justice doesn’t stop at the courtroom door. For generations, the judicial system has relied on the com-

[16] The Digital Personal Data Protection Act, 2023.

forting idea that a fair trial inside the courtroom was enough to produce a right result. But the digital age has blown that premise to pieces. For an era of the transformation of local court registries into a permanent, marketed, and globally accessible archive, the dissemination of personal identifiers without mitigation results in a sort of extrajudicial punishment that extends beyond any legal sentence or debt paid to society. The internet has converted open court records into a weapon, turning the wonderful democratic principle of judicial transparency into a tool for everlasting digital stigmatization.

As this manuscript has shown, a win for public transparency or for personal privacy is not required to resolve this crisis. The tension between these two basic ideals is an encouragement to innovation, not surrender. Modern judiciaries are capable of effectively safeguarding both the public interest and human dignity when they jettison an outdated, binary "all-or-nothing" approach to public documents and adopt the Principle of Proportional Accessibility.

THE FUTURE OF FAIR ACCESSIBILITY	
JUDICIAL TRANSPARENCY **(Protects the System)**	**RIGHT TO BE FORGOTTON** **((Protects the Person)**
• Public Precedents • Open Courtroom • Accountable Judiciaries	• De- Indexed Name Searches. • Masked Identifiers. • Automated sealing.

The structural mechanisms developed by pioneering judiciaries, as shown by the Delhi High Court's landmark 2026 judgment in **Laksh Vir Singh Yadav v. Union of India**[17], provide a clear roadmap for the future. We demonstrate that it is feasible to maintain the integrity of the law without adversely impacting the lives of ordinary citizens, through the use of a Three-Tier Access Framework, driven by targeted de-indexing and personal identity masking. This strategy retains the legal precedent for scholars, appellate courts, and legal experts, while restoring "practical obscurity" for private individuals who have earned the right to a clean slate. It assures that the law retains transparency of history, and that private, commercial platforms do not abuse human fragility as a permanent commodity.

It is time for judiciaries and legislatures around the world to act quickly to modernize open-court doctrines for the internet age. To cling to an analogue definition of transparency in a digital era is to be complicit in the systemic destruction of human rehabilitation and personal privacy. We need to establish such a system where the internet is legally compelled to forget what the law has already forgiven. If we are to ensure that the legal system serves as a tool of real healing, rehabilitation and finality, both in and beyond the courtroom, we need to modernize our public record architecture to honour the Right to Be Forgotten.

[17] .Ibid