Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The Right to Be Forgotten in Public Archives: Should Legal Databases Face Defamation Liability?

Prachi[a]

[a]Chanakya National Law University, Patna, India

Received 20 June 2026; *Accepted* 20 July 2026; *Published* 25 July 2026

Somewhere in a legal database sits a case that mattered enormously to two people once, and to almost no one since. This article asks a narrow but pressing question: when a database keeps a niche, decades-old, purely private judgment permanently searchable by name, should it bear any legal responsibility for the harm that permanence causes? The inquiry sits at the collision of two principles rarely forced to confront each other directly; the doctrine of open courts, traced here through Scott v Scott, which treats publicity as a structural check on power rather than a courtesy, and the right to be forgotten, born out of the CJEU's ruling in Google Spain and developed since through GDPR's storage-limitation principle and a still-unsettled thread of Indian High Court jurisprudence following Puttaswamy. The article argues that legal databases occupy a distinct position in this debate, different from search engines or news archives, because their claim to public-interest protection is strong for precedent-setting judgments but considerably weaker for cases involving only private parties with no lasting legal value. After weighing the case for liability against the countervailing risks to research, archival integrity, and free expression, the article proposes a graduated response rather than a binary rule, consisting of upstream redaction, de-indexing without deletion, time-based sunset provisions, and tiered liability distinguishing accurate reproduction from added commentary. It does not resolve the underlying tension, but argues the law's response should match the remedy to how much public interest has genuinely survived time.

Keywords: *right to be forgotten, open justice, legal databases, court archiving, defamation liability.*

INTRODUCTION

Somewhere in a legal database right now sits a case that once mattered enormously to two people, and to almost no one since. A dismissed defamation suit, a minor tort claim settled quietly years ago, a litigant who was never a public figure, never convicted of anything, whose only real misfortune was that a private dispute happened to produce a judgment that a search engine or legal research platform has since indexed and made permanently retrievable by name. For that person, the case isn't history. It's the first thing a prospective employer or landlord finds, long after everyone involved has moved on.

That's the quiet collision this article is really about: the principle of open courts, which has always depended on judicial records being public, running up against a person's growing claim not to be permanently defined by one obscure legal episode. For most of legal history, this tension barely surfaced in practice. Court records were technically public, but 'public' meant something very different when finding anything required a trip to a record room and the patience to dig through paper files by hand. Scholars call this quiet protective friction 'practical obscurity': the idea that information can be public in principle while remaining functionally inaccessible in practice, and that this inaccessibility does real privacy-protective work on its own, without anyone having to make a deliberate decision to seal it.[1] Digitisation has stripped that friction away almost entirely. A name search that once took an afternoon in a records room now takes a second in a browser, and it never gets tired, never loses the file, never forgets to look.

The right to be forgotten grew directly out of this shift. The CJEU's 2014 ruling in Google Spain v AEPD and Mario Costeja González held that search engines could be made, on request, to delist results linking a person's name to information that had become outdated, irrelevant, or excessive even where the underlying source stayed lawfully published.[2] The Court was careful here, and the care matters: this was about obscurity, not erasure. The newspaper notices about Costeja's old debt stayed online exactly as it always had; only its

[1] David S Ardia, 'Privacy and Court Records: Online Access and the Loss of Practical Obscurity' (2017) 5 University of Illinois Law Review 1385 <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1062&context=faculty_publications> accessed 14 June 2026

[2] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] Case C-131/12 (ECLI:EU:C:2014:317)

findability by name search was cut off.[3] That distinction between deleting a record versus simply making it harder to stumble on by name sits at the centre of almost every serious reform proposal in this space, including the one this article eventually lands on.

The picture gets messier still in the United States, which has no general right to be forgotten, and where defamation and republication law, including the fair report privilege, grew up around a different instinct entirely: protect accurate reporting of court proceedings; don't restrict it.[4] So the question this article really wants to sit with isn't the broad 'should there be a right to be forgotten,' but something narrower and harder that is, whether that existing framework, built for a different purpose, leaves any room for the specific case of 'niche' tortious defamation for real harm to an identifiable private person, against almost no public value in keeping the case findable.

Legal databases occupy an odd position that existing right-to-be-forgotten thinking wasn't really built to handle. General search engines and news archives serve broad audiences, but legal databases exist for a focused reason: to help legal professionals verify precedents and build stronger cases. That purpose gives it a genuinely strong claim to a public-interest exemption; nobody wants a legal researcher unable to find a relevant precedent because someone somewhere asked for it to be quieter. But that exemption starts to look thin exactly where this article is interested, when a case involves only private parties, has no ongoing precedential weight, and exists in the database purely because the software indexed everything it could reach. In that narrow situation, the public-interest justification is technically true but does almost no real work, while the reputational harm it enables does quite a lot.

THE DOCTRINE OF OPEN COURTS AND PUBLIC ARCHIVING

Courts settled a surprisingly old question long before anyone worried about search engines or legal databases: can justice ever happen behind closed doors? English law has stood firm on "no" for generations, with Scott v Scott serving as the definitive, uncompromising word

[3] Ignacio Cofone, 'Google v Spain: A Right to Be Forgotten?' (2015) 15 Chicago-Kent Journal of International and Comparative Law 1 <https://studentorgs.kentlaw.iit.edu/jicl/wp-content/uploads/sites/5/2015/01/Cofone-FINAL-EDIT.pdf> accessed 14 June 2026

[4] Danielle Bernstein, 'Why the "Right to be Forgotten" Won't Make It to the United States' (*Michigan Technology Law Review*, 06 February 2020) <https://mttlr.org/2020/02/why-the-right-to-be-forgotten-wont-make-it-to-the-united-states/> accessed 14 June 2026

on the matter.[5] The facts were almost mundane: a nullity petition heard in private, and a wife who later shared the transcript to defend her own name. But the House of Lords turned it into something much bigger than the facts warranted. To Viscount Haldane, public court proceedings weren't just a nice courtroom tradition but were the default rule. Closing the courtroom demanded undeniable necessity, not a judge simply deciding that privacy would be more convenient for everyone.[6] Earl of Halsbury reached even further back to make the same point, quoting an eighteenth-century lawyer who'd already noticed that English courts, unlike some of their continental counterparts, had always sat 'publicly and in open view.'[7]

Lord Shaw of Dunfermline's opinion is the one worth actually sitting with, though. He reached for Bentham's old warning that secrecy is where 'sinister interest and evil in every shape have full swing,' and that publicity is, in Bentham's words, the very soul of justice.[8] He also pulled in the historian Hallam, who'd ranked open justice as the single most important guarantee of civil liberty any country can have, more important than Parliament watching over things. What's striking, reading these judgments now, is how little the House of Lords cared about openness as a courtesy to spectators. They cared about it as a check on power. A court no one can watch, as they saw it, is a court that answers to nobody.

None of this was absolute, of course; Scott v Scott carved out a few narrow exceptions: wards of court, lunacy proceedings, trade secrets, the kinds of cases where a public hearing would destroy the very thing the case was trying to protect.[9] But the exceptions stayed narrow, and later scholarship has tracked just how carefully courts guarded against letting them creep wider. Bosland and Gill, following the doctrine forward from Scott v Scott, point out that open justice has always travelled alongside a judge's duty to give reasons publicly.[10] Rodrick takes this even closer to where this article wants to go: she argues open justice was never really just about letting people sit in the courtroom, but about being able to get the documents afterwards, because a hearing you can watch but never revisit on paper leaves almost nothing

[5] *Scott v Scott* [1913] AC 417 (HL)
[6] *Ibid* [438]–[39]
[7] *Ibid* [441]
[8] *Ibid* [477]
[9] *Ibid* [480], [482]–[83]
[10] Jason Bosland and Ashleigh Gill, 'The Principle of Open Justice and the Judicial Duty to Give Public Reasons' (2014) 38(2) Melbourne University Law Review 482 <https://findanexpert.unimelb.edu.au/scholarlywork/967376-the-principle-of-open-justice-and-the-judicial-duty-to-give-public-reasons> accessed 14 June 2026

behind for real scrutiny.[11] That distinction of watching versus retrieving turns out to matter far more than anyone in 1913 could have anticipated.

Because here's where the doctrine starts to strain. It was built for a world where "public" came with built-in friction. Getting at a record meant physically going somewhere, asking someone, sitting down with paper files. Scholars have a name for that friction now: "practical obscurity", the idea that something can be public in theory while staying just inaccessible enough in practice that the inaccessibility itself quietly protects people, without anyone ever deciding to protect them. Scott v Scott never had to reckon with that friction disappearing, because in 1913 it hadn't yet. Nobody could type a name into a search bar and pull up a century-old nullity suit in under a second. The whole doctrine assumed that finding anything would always cost somebody a bit of effort.

That assumption is exactly what digitisation quietly wiped out, and more recent writings are calling it out directly. Historically, legal privacy was protected by simple inconvenience: having to travel to a courthouse and dig through paper files kept most people from prying. When court records went online, that accidental shield disappeared. The CanLII article argues that making records instantly searchable isn't a harmless upgrade, and courts now need to deliberately put some of that friction back to protect personal privacy.[12] The principle itself hasn't moved an inch; open justice as a check on power is exactly what it always was. What's moved is how far that openness can now follow one ordinary, powerless person, for the rest of their life, long after anyone with a legitimate reason to care has stopped caring. That gap between what the doctrine was built to do and what it now quietly does instead is exactly where the collision with the right to be forgotten begins.

---

[11] Sharon Rodrick, 'Open Justice, the Media and Avenues of Access to Documents on the Court Record' (2006) 29(3) University of New South Wales Law Journal 90 <https://20.austlii.edu.au/cgi-bin/viewdoc/au/journals/UNSWLawJl/2006/40.html> accessed 14 June 2026

[12] Jane Bailey and Jacquelyn Burkell, 'Revisiting the Open Court Principle in an Era of Online Publication: Questioning Presumptive Public Access to Parties' and Witnesses' Personal Information' (2017) 48(1) Ottawa Law Review <https://www.canlii.org/en/commentary/doc/2017CanLIIDocs166#!fragment//BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoByCgSgBpltTCIBFRQ3AT0otokLC4EbDtyp8BQkAGU8pAELcASgFEAMioBqAQQByAYRW1SYAEbRS2ONWpA> accessed 14 June 2026

ORIGIN AND SCOPE OF THE RIGHT TO BE FORGOTTEN

The concept of the "Right to Be Forgotten" in digital jurisprudence largely owes its modern origin to the landmark European Court of Justice ruling in Google v Spain. In this case, Mario Costeja González had settled that debt long before anyone raised the matter again. The old newspaper notice announcing the original property auction, though, had never gone anywhere; it just sat online, and Google's search engine kept surfacing it every time his name was searched. Costeja didn't ask the newspaper to remove the article. He asked Google to stop linking his name to it. In 2014, the Court of Justice of the European Union agreed, and in doing so created something genuinely new: a right to have search results delisted, even where the underlying source stayed online and stayed entirely lawful.[13] The Court carefully preserved a critical distinction regarding the newspaper article, which remained unchanged in its original form. Instead, the legal focus shifted to how search engine mechanics made the article easier to locate via name searches. That's the core idea in miniature: not erasing the past, just switching off the spotlight that used to follow it around automatically.

The right didn't stay frozen at that single ruling. A few years later, in GC and Others v CNIL, the CJEU had to work out how the right behaved when the information involved was genuinely sensitive, such as criminal history, political opinions, and similarly protected categories of data.[14] The Court held that a search engine doesn't have to independently verify every underlying fact before agreeing to delist; it's enough that the person requesting delisting shows the data is inaccurate, outdated, or excessive, at which point a proper balancing exercise between privacy and public interest needs to follow. In the companion case, Google LLC v CNIL, the Court addressed a more practical question: does a European delisting order apply everywhere, or only within Europe? The answer was that EU law doesn't require worldwide delisting; de-referencing has to happen across EU member states, but nothing in EU law compels Google to apply it globally. That ruling quietly drew a border around a right that otherwise sounds borderless, and it's a detail worth remembering later, since geography turns out to matter enormously once the question becomes focused on who needs to view and use the legal database's records.

[13] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] Case C-131/12 (ECLI:EU:C:2014:317)
[14] *GC and Ors v Commission nationale de l'informatique et des libertés (CNIL)* [2019] Case C-136/17 (ECLI:EU:C:2019:773)

Things look completely different once you leave Europe. The United States has deliberately avoided creating anything like a 'right to be forgotten.' That isn't an accident; American free speech and defamation laws are built on the exact opposite idea, where publishing accurate information matters more than suppressing it. Because there is no real legal foundation for hiding records in the US, legal debates there usually focus on much tighter rules, like the fair report privilege, rather than a sweeping right to erase the past.

India sits somewhere between these two poles. It has no standalone statutory right to be forgotten currently in force. What it does have is Justice K.S. Puttaswamy v Union of India, the 2017 nine-judge bench ruling that recognised privacy as a fundamental right under Article 21 of the Constitution.[15] The judgment didn't announce a right to be forgotten by that exact name. Still, it spent real time on informational privacy and the unusual permanence of the digital age, leaving the door open for a doctrine like this to develop later.

Since Puttaswamy, individual High Courts have picked up that thread, and not always in the same direction. The Karnataka High Court, in Sri Vasunathan v Registrar General, allowed a woman's name to be masked from a judgment involving her acquittal, reasoning that her privacy interest outweighed whatever public value remained in keeping her name permanently attached to a case where no wrongdoing was ever found.[16] Years later, the Madras High Court had to sit with a strikingly similar question and landed in two different places within the same case. A man named Karthick Theodore, acquitted on appeal after an earlier conviction, asked the Court to have his name stripped from the judgment recording the whole episode. A single judge said no.[17] But a Division Bench of the same High Court, hearing his appeal, disagreed and directed that his name be removed from the version of the judgment held by the online legal database Indian Kanoon.

That disagreement, sitting inside one case, is really the whole story of the right to be forgotten law of India in miniature right now. Judges can look at a regular person's decades-old legal mistake and still decide that the public has a right to know their identity. Another bench, looking at the same facts, can see nothing left worth protecting except his privacy. Yet neither view has been declared wrong by anything above. This is an accurate description of where

[15] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[16] *Sri Vasunathan v Registrar General* (2017) SCC OnLine Kar 424
[17] *Karthick Theodore v Registrar General* (2021) SCC OnLine Mad 2755

Indian law on this exact question currently stands: recognised in principle since Puttaswamy, but still being worked out High Court by High Court, case by case, without a single settled national answer. Which is, in its own way, the perfect setup for the question this article is actually asking. In the absence of uniform judicial standards regarding retroactive case anonymisation, commercial legal databases lack both the institutional mandate and the due process mechanisms required to balance privacy claims against public access.

LEGAL DATABASES AS A DISTINCT CATEGORY

Specialised legal databases such as LexisNexis, Westlaw, or open-access repositories like Indian Kanoon and CanLII occupy a unique place in the digital information ecosystem, distinct from general search engines and news archives. While general search engines process web content for everyday consumer queries, legal databases curate primary legal sources specifically to advance legal research, institutional transparency, and the doctrine of precedent. They fulfil the constitutional imperative of open justice, ensuring that court judgments remain accessible to legal professionals, scholars, and the general public.[18] Consequently, publication in a dedicated legal repository carries an expectation of permanence and fidelity to the official record; in contrast, indexing on commercial search engines creates broad, incidental exposure to lay audiences who may consume judicial information without legal context.

This distinction becomes particularly contentious in cases involving low-profile private litigants. Unlike public officials or corporate entities, ordinary citizens drawn into minor criminal trials or private litigation often face long-term reputational harm when their full names remain indexed on public legal databases. Even when an individual is fully acquitted, or a matter is resolved out of court, search engine indexing ensures that a simple name lookup by prospective employers or landlord background checks brings up past litigation. In these scenarios, the persistent public indexing of minor or resolved records yields minimal public-accountability value while inflicting disproportionate, lifelong harm on an individual's personal and professional standing.

[18] *Nixon v Warner Communications, Inc* (1978) 435 US 589

To determine whether legal databases should bear legal responsibility for hosting such damaging information, courts and scholars evaluate three distinct legal liability frameworks:

The foundational defence for legal databases is the fair report privilege, often understood alongside qualified privilege. Under this doctrine, entities that accurately reproduce official public records or court proceedings without malice are shielded from defamation liability, even if the underlying judicial record contains false or defamatory allegations.[19] Because legal repositories merely mirror official court dockets, their publication of unedited judgments traditionally receives robust protection under the principle that the public has a right to know what transpires within the judicial system.[20]

Where defamation or privacy claims extend beyond common law privileges, legal databases frequently rely on statutory intermediary immunity. Under provisions such as Section 230 of the Communications Decency Act in the United States,[21] Section 79 of the Information Technology Act 2000 in India,[22] and Article 6 of the EU Digital Services Act,[23] digital platforms are exempt from liability for third-party content, provided they act as passive hosts and satisfy prescribed due-diligence or take-down obligations. Under these safe-harbour regimes, a database that automatically ingests and displays public court decisions functions as an intermediary rather than a primary publisher, immunising it from direct liability for the content of those decisions.

However, this statutory immunity is not absolute and shifts toward direct publisher liability if a database alters its role. When a legal repository moves beyond passive indexing by adding editorial commentary, drafting summaries, creating custom headnotes, or applying selective metadata tags that misrepresent or highlight defamatory aspects of a case, it may lose its safe-harbour protections.[24] By actively shaping or contextually altering the presentation of judicial information, the platform assumes an authorial role, exposing itself to strict publisher liability under standard tort law principles.

[19] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [298]–[300]
[20] *Restatement (Second) of Torts § 611* (American Law Institute 1977)
[21] Communications Decency Act 1996 (47 USC s 230)
[22] Information Technology Act 2000, s 79
[23] EU Digital Services Act 2021, art 6
[24] Information Technology Act 2000, s 79

WEIGHING THE CASE FOR AND AGAINST LIABILITY

Having laid out how legal databases actually work, and what protects them under existing law, it's worth pausing to ask the harder normative question directly: even if databases can currently avoid liability for hosting a niche, decades-old defamation case, should the law let them keep doing so indefinitely? The honest answer is that both sides of this argument are genuinely strong, which is exactly why the tension hasn't resolved itself anywhere in the world.

The primary argument for hiding online court records is that public interest decreases over time while personal harm increases. Whatever public interest existed in a case when it was decided doesn't stay constant forever; it fades, and it fades at very different speeds depending on who's involved. A case concerning a sitting politician, a public company, or an ongoing pattern of misconduct might reasonably stay relevant for decades. A case involving a private, non-public individual, someone who was never a party of continuing interest, who was acquitted, whose civil dispute was quietly settled, or who was simply a peripheral figure in someone else's litigation, loses whatever public value it had far more quickly, often within a few years of the judgment being handed down. Once that public interest has genuinely faded, continuing to keep the case permanently searchable by name isn't preserving accountability; it's just attaching a stale label to someone's identity that no longer serves the purpose the open-courts principle was built to protect in the first place.

Beyond time, digital permanence scales up the problem by actively transforming the meaning and impact of old information. A single court appearance, however minor, however long ago, however resolved, becomes the very first thing anyone learns about a person the moment they search that person's name. That's a genuinely new kind of harm that the old open-courts doctrine was never designed to anticipate, because it assumed that continued visibility would always require real effort to find. Once that cost drops to zero, a single episode risks becoming a person's entire searchable identity, disproportionate to how much that episode actually says about who they are.

This is precisely the reasoning that has already produced binding law elsewhere, and it's worth taking seriously as more than just theory. Article 17 of the GDPR gives individuals a directly enforceable right to have personal data erased once it is no longer necessary for the purpose for which it was originally collected, which is essentially the proportionality argument written into statute.[25] The Belgian Court of Cassation went even further than a mere search-delisting remedy in Olivier G v Le Soir, upholding an order requiring a newspaper to actually anonymise its own online archive of a 1994 article about a fatal drink-driving accident, on the basis that keeping the applicant's name attached to the story decades later caused him harm disproportionate to whatever remained of the newspaper's freedom of expression once his sentence had been served and his conviction had become spent.[26] That case matters a great deal for this article specifically, because it shows a European court willing to order changes to an archive itself, not merely to how a search engine indexes it, which is a much closer analogy to what a legal database liability regime would actually require. And underlying both of these developments is the reasoning the CJEU first set out in Google Spain, that continued digital accessibility of personal information can become excessive and outdated even where the original publication was entirely lawful, justifying a delisting remedy that leaves the underlying record intact.[27]

And yet, the case against imposing liability on legal databases is just as serious, and arguably harder to argue around. Legal databases exist because lawyers, researchers, journalists, and ordinary citizens genuinely need to find precedent, verify claims, and conduct due diligence, checking a potential business partner's litigation history, screening a job candidate, or running a conflict check before taking on a new client. Every one of those legitimate uses depends on a database being comprehensive rather than selectively curated to surface what individual subjects would prefer to see surfaced. If databases start proactively removing or masking cases whenever the subject requests it, the predictable result is a chilling effect that runs in the opposite direction from what right to be forgotten proponents intend: researchers stop trusting that any given database is actually complete, which pushes serious users back toward manually compiling records from primary court sources, recreating exactly the inefficiency and cost the digitization of legal records was supposed to eliminate in the first place.

[25] General Data Protection Regulation 2016, art 17
[26] *Olivier G v Le Soir,* Cour de Cassation Belgique, Apr 29, 2016, N° C.15.0052.F (Belgium)
[27] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] Case C-131/12 (ECLI:EU:C:2014:317)

Beyond just the practical side of things, there is a separate, deeper point to be made about archival integrity. Courts, and the archivists and databases that preserve their output, have a longstanding institutional duty to maintain the historical record intact and accurate, not just for today's readers but for future historians, policymakers, and litigants who may need to trace how the law, or a particular pattern of conduct, actually developed over time. Selectively editing that record after the fact, however sympathetic the individual request, risks quietly rewriting legal history one case at a time, with no consistent principle governing which cases get preserved and which get quietly erased.

Then there's the unworkability problem, which is less about principle and more about practical mechanics. Even if everyone agreed that 'niche' cases involving purely private individuals deserve different treatment from precedent-setting or genuinely newsworthy ones, someone still has to decide, case by case, which category any given judgment falls into. A legal database is not a court, has no adjudicative process, and has no obvious way of determining fairly and consistently across millions of records without either over-removing cases that still have real value, or under-removing cases that cause genuine harm. When we delegate this gatekeeping authority to private corporations instead of the judiciary, which is specifically structured to balance these conflicting rights, we risk transforming databases into unaccountable censors. These companies end up making quiet, unilateral choices about which histories deserve preservation and which can be erased, completely bypassing legal oversight.

Finally, in jurisdictions with strong constitutional protection for the press, there's a direct legal counterweight to nearly everything argued above. The U.S. Supreme Court held in Cox Broadcasting Corp v Cohn that the First Amendment protects your right to share accurate information from public court files. Because what happens in court impacts everyone, the law cannot punish you for republishing those open records.[28] It reaffirmed and extended that reasoning in Florida Star v BJF, holding that even highly sensitive information, in that case, a sexual assault victim's identity, cannot be the basis for civil liability against a publisher who obtained it lawfully and reported it accurately, unless the state can show that liability serves an interest of the very highest order, narrowly and evenhandedly applied.[29] Read together,

[28] *Cox Broadcasting Corp v Cohn* [1975] 420 US 469

[29] *Florida Star v BJF* [1989] 491 US 524

these cases suggest that in the United States, constitutional protections for free speech and public information largely safeguard platforms that publish accurate court judgments, even when individuals claim reputational harm.

The debate between data privacy and public access requires a balanced middle ground, as both corporate liability and public exposure have compelling arguments depending on the context. Liability is most logical for minor, private, and obsolete records, while protecting access is crucial for active journalism, research, and background checks.

THE PATH FORWARD

Everything argued so far points to the same uncomfortable truth: neither 'hold legal databases fully liable' nor 'give them blanket immunity' is a satisfying answer to the niche defamation problem this article set out to examine. But refusing to pick a side isn't really an option either, so it's worth landing somewhere more specific than simply restating that both sides have a point.

The most promising starting point sits upstream of the database entirely. Ardia's proposal that courts should limit what enters the public record in the first place, rather than leaving the clean-up to whoever hosts it afterwards, deserves to be the first line of defence. A database cannot un-know what a court has already published, but a court can be far more careful about what it publishes, particularly where a case turns on facts about a private, non-party individual with no real bearing on the legal reasoning. If fewer defamatory or needlessly identifying details entered the public record in the first place, the entire downstream question of database liability would shrink considerably, simply because there would be less to fight over later.

Where that fails, de-indexing rather than deletion is the next best option, the remedy the CJEU settled on in Google Spain.[30] The judgment never touched the underlying record; it only removed the ability to find it through a name search. This approach sidesteps subjective evaluations of merit, focusing instead on the practical distinction between locating individuals by name versus identifying topics by subject, with the latter requiring long-term

[30] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] Case C-131/12 (ECLI:EU:C:2014:317)

persistence. Consequently, only the thematic, subject-based content necessitates permanent findability rather than personal identifying information.

Time is the third lever. A precedent-setting judgment should stay fully discoverable indefinitely, since its value doesn't fade with age. A judgment whose relevance was always confined to two private parties, with no precedential weight, could reasonably carry a sunset period after which name-based indexing lapses automatically, absent a demonstrable ongoing public interest. This isn't a novel idea; it mirrors the storage-limitation principle already built into data protection law, which ties retention to how long data remains necessary for its original purpose.[31] India's own data protection statute gestures toward something similar, giving individuals a right to request erasure once that purpose has been served, even without using the phrase 'right to be forgotten' anywhere in its text.[32]

The last piece is a line drawn through the database's own conduct rather than through the case itself: no liability for accurately reproducing a judgment as issued, but real liability where a database adds commentary or labelling that amplifies the harm beyond what the court actually said. This tracks how intermediary immunity already works in the United States: Section 230 protects platforms because they aren't treated as authors of content that originated elsewhere, and Zeran read that protection broadly for exactly that reason.[33] That logic weakens when platforms move from neutral hosting to active content curation, such as mislabeling a dismissed case as a 'fraud case'. By actively shaping information, the system shifts from a passive conduit to a contributor to harm.

None of these four ideas is complete on its own. Upstream redaction depends on judicial discipline that varies by court. De-indexing requires real technical infrastructure. Sunset clauses still require someone to decide which cases count as non-precedential. Tiered liability requires courts to draw a workable line between reproduction and commentary. But together these solutions shift the focus away from a strict, all-or-nothing approach, promoting a nuanced strategy instead. This method aligns legal remedies with the actual level of enduring public interest as time passes.

[31] General Data Protection Regulation 2016, art 5(1)(e)
[32] Digital Personal Data Protection Act 2023 (India), s 12(3)
[33] *Zeran v America Online Inc* [1997] 129 F 3d 327 (4th Cir 1997); Communications Decency Act 1996

That is the thesis this article has been building toward. The collision between open courts and the right to be forgotten isn't a sign that one principle is wrong and the other right. Open justice matters exactly as much today as when Scott v Scott insisted on it over a century ago, a check on power that depends on courts being watchable.[34] But the right to be forgotten isn't really an attack on that principle; it's a response to something Scott v Scott never had to anticipate: that watching a court used to cost something, and now it doesn't. The hard tradeoff this article keeps returning to, between a private individual's interest in not being permanently defined by one old case and the public's interest in a complete legal record, doesn't resolve cleanly in either direction, and an honest article has to admit that rather than paper over it with a tidy conclusion.

The future of this law isn't going to change overnight with one massive rule, delivered by one court, in one dramatic ruling. It will be built the way most real legal change actually happens: in fragments, unevenly, one jurisdiction nudging the balance a little further than the last, the way Scott v Scott did for open justice, the way Google Spain did for search engines, the way India's High Courts are doing right now, case by case. Somewhere in that slow, uneven process is a version of the law that finally treats an old, obscure case for what it actually is, not a permanent verdict on who a person is, and not a piece of history anyone has the right to erase, but something in between, deserving of a little less certainty than either side of this debate would like to admit. Until that version of the law arrives, the person whose case opened this article, the one whose entire searchable identity is still one dismissed dispute from a decade ago, is left waiting on a legal system that hasn't yet decided whether it owes them anything at all.

[34] *Scott v Scott* [1913] AC 417 (HL)