



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

INJURY WITHOUT LOSS: LOCATING THE COMPENSABLE HARM IN DATA BREACH LITIGATION ACROSS THREE JURISDICTIONS

AUTHORED BY - ISHIKA ISHANVI & NITISHA HANSDAH

Abstract

Data breach litigation raises a difficult question: what is the injury when personal information is exposed but no financial loss follows? This article compares the United States, the United Kingdom and India and argues that their divergence is structural rather than a matter of relative generosity. Each system applies a decisive filter at a different stage. In the United States the filter operates at the threshold, through Article III standing: after *TransUnion v Ramirez*, exposure alone is not an injury in fact. The United Kingdom filters through proof and procedure: *Lloyd v Google* requires individualised proof and *Warren v DSG* closes the equitable routes for negligent security, although *Farley v Paymaster* has partly reopened the field. India filters at the remedy: the Digital Personal Data Protection Act 2023 provides for penalties but gives data principals no right to compensation. The article argues that these filters have the same effect, containing indeterminate liability, and that their deepest effect is on aggregation rather than on individual claims. It concludes by assessing reforms, including statutory damages and a compensation fund financed from DPDP penalties.

Keywords: data breach; compensable harm; Article III standing; collective redress; Digital Personal Data Protection Act 2023.

I. Introduction

A data breach is, in the ordinary case, an event that leaves no trace on the claimant's bank balance. A hospital's records are exfiltrated; a retailer's payment system is compromised; a government portal exposes identification numbers to anyone who guesses a URL. Months pass and no fraudulent transaction appears. The claimant knows only that information she gave in confidence is now in hands she cannot identify, for purposes she cannot predict, for a duration that has no end. She sues. The defendant answers that she has lost nothing.

That answer is not frivolous. Compensatory tort law is organised around restoring a position

disturbed by a wrong, and restoration presupposes a disturbance capable of measurement. Where the wrong consists in the loss of control over information, the disturbance resists that logic in three ways at once. It is prospective, in that the injury feared is misuse that has not yet occurred and may never occur. It is probabilistic, since the claimant cannot say whether her particular record was among those actually read, and the defendant frequently cannot say either. And it is dignitary, because the complaint is not that something was taken but that something was seen, a species of injury the common law has compensated only in narrow and well-policed categories.

Courts in every jurisdiction with a mature data protection regime have had to decide how much of this to admit, and they have diverged sharply while facing materially identical litigation. The same breach, pleaded on the same facts by claimants with the same grievance, produces a dismissal for want of constitutional standing in a United States federal court, typically a strike-out in the English High Court, and in India little prospect of compensation from a private defendant, whatever the constitutional status of the interest.

This article argues that the divergence is not a matter of judicial temperament or of some jurisdictions being more generous than others. It is structural. Each system applies a decisive filter, but each applies it at a different stage of the litigation, and the stage at which a system filters reveals what it understands data protection law to be doing. The United States filters at the threshold, the United Kingdom at proof and procedure, and India at the remedy.

Part II constructs a taxonomy of the harms claimants actually plead, a necessary preliminary because the three jurisdictions do not disagree about data breaches in the abstract; they disagree about which pleaded injuries count. Parts III to V examine the three systems in turn. Part VI draws the filters together and asks which institution is trusted to decide that exposure alone is not enough. Part VII explains why breach harm fits tort so badly. Part VIII shows that the injury requirement's deepest effect is on aggregation. Part IX evaluates reform, and Part X concludes.

II. What Claimants Allege: A Taxonomy of Breach Harms

Comparison requires a common object, and the pleadings are remarkably uniform across jurisdictions even where the outcomes are not. Six categories recur, ordered here by their distance from conventional pecuniary loss. At one end sits pecuniary loss already suffered: funds withdrawn, a credit line opened in the claimant's name, a tax refund diverted. This is uncontroversial everywhere and also the rarest. Its difficulty is almost never recognition of the harm but attribution, since a claimant whose details appear in four separate breaches in a single

year faces a causation problem no theory of injury can solve for her.

Slightly further out lies mitigation expenditure like credit monitoring, replacement card fees, the cost of a credit freeze, time spent on remedial administration. These are real outlays, yet they are contested because they are self-incurred. The claimant chose to spend in response to a risk, so whether the expenditure is compensable depends entirely on whether the underlying risk was itself an injury. A jurisdiction that denies the risk treats the expenditure as a voluntary cost rather than a loss.

The third category, and the most contested, is the claim that exposure has raised the probability of identity theft even where none has occurred. Risk is continuous while liability is binary, so recognising it demands that courts fix a threshold of probability at which a contingency becomes an injury. Neither any increase in risk nor virtual certainty is a workable line, and everything between is a matter of degree dressed up as a matter of kind.

Claimants also plead emotional distress such as anxiety, sleeplessness, the specific fear that one's information is circulating among people who intend to use it. Common law systems have been wary of distress unaccompanied by physical injury or a recognised psychiatric condition, chiefly from concern about verification and indeterminate liability. Data protection statutes have displaced that wariness by express provision, which largely explains why distress claims have fared comparatively well in Europe and badly in the United States.

More ambitious is the contention that the claimant has been deprived of something valuable in itself, authority over the circulation of information about herself, regardless of any consequence. This loss-of-control theory is the most attractive of the categories to claimant representatives because it is the only one uniform across a class, and therefore the only one that makes mass litigation feasible without individual assessment. That same feature is exactly what caused its rejection in *Lloyd v Google*, discussed in Part IV.

Finally, there is informational injury, the theory that where a legislature confers a right to have one's data handled in a particular manner, denial of that right is itself the injury. This differs in kind rather than degree. The first five categories describe states of the claimant; this one describes a state of the defendant's compliance, and asks the court to treat non-compliance as actionable without more.

The pattern of acceptance and rejection tracks a prior commitment about what the law is for. A system that sees tort as restoring losses accepts the first two categories and resists the last three. A system that sees data protection as a regulatory regime enforced partly by private action accepts the sixth. A system that treats informational privacy as dignity or autonomy accepts the fifth.

III. The United States: Standing as the Gatekeeper

The American law of breach harm is distinctive because the decisive question is not whether the claimant has a good cause of action but whether a federal court has power to hear her at all. Article III confines the judicial power to cases and controversies,¹ and the Supreme Court has construed that limitation to require an injury in fact that is concrete and particularised and either actual or imminent, fairly traceable to the defendant's conduct, and likely to be redressed by a favourable decision.

The consequence is a filter with no counterpart in England or India. An English court asked whether distress is compensable is asking about the content of a statutory remedy, and Parliament may answer it. An American federal court asking whether a statutory violation is an injury in fact is asking about the limits of its own constitutional authority, and Congress may not answer it.

The trilogy

The vocabulary now used in breach cases was supplied by a decision that was not about a breach at all. In *Clapper v Amnesty International USA*, the Court held that threatened injury must be certainly impending, and that an objectively reasonable likelihood of future harm would not suffice.² It added, in a footnote that has done considerable work since, that claimants cannot manufacture standing by inflicting costs on themselves in response to a risk that is not itself cognisable. That footnote is why mitigation expenditure cannot stand as an independent injury in federal court: it is parasitic on the risk and falls with it.

The informational injury theory was taken up three years later in *Spokeo Inc v Robins*, where the Court held that concreteness and particularisation are distinct requirements and that a bare procedural violation divorced from concrete harm does not satisfy Article III.³ The decision generated a decade of inconsistent application, in part because the Court conceded both that intangible harms may be concrete and that risk can sometimes satisfy the requirement, without specifying when either concession applies.

Much of that ambiguity was resolved, restrictively, in *TransUnion LLC v Ramirez*.⁴ The majority's formulation that there is no standing without concrete harm came with a methodology: an intangible injury is concrete if it bears a close relationship to a harm traditionally recognised as providing a basis for suit. The analytical move lies in the treatment of the class. The claimants were consumers whose credit files had been incorrectly flagged as potential terrorist matches, and the Court divided them. For those whose files had actually been

disseminated to third parties it found an analogue in defamation and upheld standing; for the larger group whose files had been compiled but never disclosed it found none, holding that inaccurate information sitting in a database, seen by nobody, resembles no traditional harm. The implication is severe. Exposure standing alone is not an injury. A claimant must plead dissemination, misuse, or a risk imminent enough to satisfy *Clapper*, and the Court indicated that in a damages action the risk of future harm will rarely suffice on its own.

The circuit split

Below the Supreme Court the federal appellate courts remain divided on when breach-induced risk is imminent enough, and the division is best understood as disagreement about inference from facts rather than about law. On the permissive side, the Seventh Circuit in *Remijas v Neiman Marcus Group*⁵ and the Sixth Circuit in *Galaria v Nationwide Mutual Insurance*⁶ reasoned that where hackers deliberately targeted and obtained personal data the natural inference is that they intend to use it. On the restrictive side, the Third Circuit in *Reilly v Ceridian*,⁷ the Fourth in *Beck v McDonald*⁸ and the Eighth in *In re SuperValu*⁹ declined that inference, requiring evidence that the data had actually been accessed or misused. Two variables sort most cases: whether the breach was targeted rather than incidental, a stolen laptop supporting a weaker inference of criminal purpose than an intrusion into a payment system, and whether misuse has already begun for some class members.

The escape routes

Article III binds federal courts. It does not bind state courts, which may adopt more permissive standing rules as a matter of state law. In *Rosenbach v Six Flags Entertainment Corp* the Illinois Supreme Court held, construing the Biometric Information Privacy Act, that a person whose statutory rights are violated is an aggrieved person entitled to sue without alleging further injury¹⁰ — precisely the informational injury theory the federal courts had been narrowing. A second route is statutory damages, which remove the need to prove individual loss; Part IX returns to it.

The interaction with *TransUnion* produces an outcome difficult to defend on any theory. A breach class action filed in or removed to federal court may now be dismissed for want of standing, and dismissal for want of jurisdiction is not an adjudication on the merits, so the proper disposition is frequently remand to state court rather than termination. The restrictive federal doctrine does not eliminate the litigation. It relocates it, to fora often more favourable to claimants, less equipped for aggregate litigation, and incapable of producing the nationwide

resolution the federal class action was designed to deliver.

IV. The United Kingdom: From Distress to Procedure

English law reached a generous conception of breach injury and then built a set of filters that rendered that generosity largely academic for low-value mass claims, until *Farley v Paymaster* partly reopened the field. The filters lie not in standing, which English law does not deploy as a constitutional device, but in the measure of damages, the availability of particular causes of action, and the power to strike out claims as an abuse of process.

Expansion, and the turn in Lloyd

Vidal-Hall v Google Inc was the turning point in the claimant's favour.¹¹ The Court of Appeal held that misuse of private information is a tort rather than an equitable claim and disapplied the statutory requirement that damage precede an award for distress under the Data Protection Act 1998.¹² Distress alone could now ground a claim, and the working assumption that followed was that distress and loss of control could be claimed per capita, without individual proof, and aggregated through a representative action.

That assumption was tested in *Lloyd v Google LLC*.¹³ The claim was a representative action under what is now CPR 19.8,¹⁴ brought for several million iPhone users whose browsing data had been collected through a workaround of Safari's cookie-blocking defaults. Because a representative action requires the represented class to share the same interest, the claim could proceed only if damages were assessed uniformly, which meant a lowest common denominator tariff: a fixed per capita sum for loss of control, claimed without evidence of distress or consequence for any individual. The Supreme Court rejected it. On the construction of the 1998 Act, damage meant material damage or distress and did not extend to the infringement itself; the statutory regime-imposed obligations whose breach required proof of resulting damage, and the claimant could not recover without evidence of what unlawful processing had actually occurred in each case.

Lloyd is therefore not best read as holding that loss of control is never an injury. It holds that loss of control cannot be presumed and standardised across a class. Since individualised proof is precisely what mass low-value litigation cannot economically supply, the decision terminated the representative-action route in this field as a practical matter.

De minimis and the closing of the equitable routes

A parallel line of first-instance authority addressed the individual low-value claim, typically a

misdirected email. In *Rolfe v Veale Wasbrough Vizards LLP* the court granted summary judgment against claimants whose data had been sent to a wrong address and promptly deleted, observing that the law does not concern itself with trivialities and that no person of ordinary fortitude would have suffered material distress.¹⁵ *Johnson v Eastlight Community Homes Ltd* went further, treating a claim arising from a brief erroneous disclosure as an abuse of process and criticising its issue in the High Court rather than the small claims track.¹⁶ These decisions must now be read with *Farley*: no de minimis threshold applies under the UK GDPR, so the *Rolfe* line survives chiefly for misuse of private information.

Warren v DSG Retail Ltd completed the enclosure.¹⁷ The claimant had pleaded breach of confidence and misuse of private information alongside the statutory claim, a strategy adopted chiefly because those causes of action attracted after-the-event premiums and success fees recoverable from the defendant, which the statutory claim did not. The court struck them out on the ground that both require a positive wrongful act. A failure to keep data secure, permitting a third party to obtain it, is neither a misuse nor a disclosure by the defendant; negligent security is an omission, and these causes of action do not lie for omissions. The consequence is that a breach claimant in England is confined to the statutory route under the UK GDPR and the Data Protection Act 2018,¹⁸ the route with the least favourable costs treatment and, after *Lloyd*, the strictest requirement of individual proof.

Article 82 and the partial reopening

Article 82 UK GDPR provides a right to compensation for material or non-material damage, and its interpretation at the Court of Justice remains persuasive though no longer binding after withdrawal. In *Osterreichische Post* the Court held that mere infringement does not of itself confer a right to compensation, while refusing to import any threshold of seriousness, so that minor but demonstrated non-material damage remains compensable.¹⁹ In *VB v Natsionalna agentsia za prihodite* it accepted that a data subject's fear of potential future misuse may itself constitute compensable non-material damage, provided the fear is well founded on the facts.²⁰ The English position changed in *Farley v Paymaster (1836) Ltd*.²¹ Pension statements for several hundred police officers had been posted to outdated addresses, and the claims were struck out below because no third party was shown to have opened the envelopes. The Court of Appeal allowed the appeal, holding that proof of disclosure to a third party is not an essential element of a UK GDPR claim, that no de minimis or seriousness threshold applies to non-material damage under that regime, and that fear of misuse is compensable where objectively well founded rather than speculative. The seriousness threshold survives in misuse of private

information.

England therefore combines a broad conception of injury with a procedural gate that has moved rather than disappeared. Distress and well-founded fear are compensable and no seriousness threshold applies under the UK GDPR. What remains is the requirement of individual proof, which *Lloyd* made decisive for representative actions, the closure of the equitable routes for negligent security, and the de minimis line in misuse of private information. The injury is no longer denied in principle; for low-value mass claims it is denied a collective vehicle.

V. India: Liberal Standing, Absent Remedy

India presents the mirror image of the American position, and the inversion is instructive precisely because it cannot be explained by any lack of commitment to privacy as a value. Indian constitutional law recognises informational privacy in emphatic terms, Indian standing doctrine is the most permissive of the three by a wide margin, and the legislature has nonetheless constructed a data protection statute that gives the individual whose data is breached no right to compensation at all.

Constitutional foundation and permissive standing

Justice KS Puttaswamy (Retd) v Union of India established, by a unanimous nine-judge bench, that privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and of the freedoms guaranteed by Part III.²² The judgment identified informational privacy as a facet of that right and acknowledged that dangers arise from both state and non-state actors. The difficulty for breach litigation is horizontality. Part III rights are generally enforceable against the State and its instrumentalities, while the overwhelming majority of breaches involve private entities: banks, hospitals, payment processors, platforms. Indian courts have developed doctrines of indirect horizontal effect, and the expansive reading of State under Article 12 captures some private bodies discharging public functions, but neither route delivers a general private law of breach compensation.

Where a claim does lie against the State the procedural position is strikingly open. Writ jurisdiction under Articles 32 and 226 operates without the constraints of Article III, and public interest litigation has relaxed the requirement of personal aggrievement almost to vanishing. The constitutional tort line beginning with *Rudul Sah v State of Bihar* establishes that the Supreme Court and High Courts may award monetary compensation in writ proceedings for violation of fundamental rights, as a public law remedy distinct from private damages.²³ An Indian court faces no equivalent of the *TransUnion* inquiry: it need not ask whether the injury

has a common law analogue, nor whether the claimant is sufficiently aggrieved.

Section 43A and the architecture of the 2023 Act

The only genuinely compensatory statutory provision India has had in this field was section 43A of the Information Technology Act 2000.²⁴ It made a body corporate possessing sensitive personal data, which was negligent in implementing reasonable security practices and thereby caused wrongful loss or wrongful gain, liable to compensate the person affected. The 2011 Rules supplied the content of the standard, specifying categories of sensitive data and requiring a documented security programme.²⁵ The provision was imperfect: confined to sensitive personal data, requiring proof of negligence and wrongful loss, and adjudicated before an Adjudicating Officer in practice slow and inconsistently resourced. But it was a right to compensation vested in the individual, and it was the only one. The Digital Personal Data Protection Act 2023 provides for its omission, but that omission, like the Act's penalty and data-principal provisions, takes effect only on 13 May 2027 under the staggered commencement notified with the DPDP Rules 2025 on 13 November 2025.²⁶

The omission is not an oversight, and this is the point on which the Indian position must be assessed. The Act establishes a Data Protection Board empowered to inquire into breaches and impose monetary penalties on data fiduciaries, with a schedule prescribing substantial maxima.²⁷ Those penalties are credited to the Consolidated Fund of India.²⁸ The data principal receives nothing. She is given a right to information, to correction and erasure, to grievance redressal and to nominate, but no right to damages; she is additionally burdened with duties, including a prohibition on registering false or frivolous grievances, backed by penalty.²⁹ This departs deliberately from the earlier drafts, since both the Srikrishna Committee's 2018 draft Bill³⁰ and the Personal Data Protection Bill 2019³¹ contemplated compensation to the data principal. Their removal reflects a considered choice to treat data protection as public regulatory enforcement rather than private vindication: the fiduciary answers to the regulator and the regulator to the State, with the individual appearing as the occasion for enforcement rather than its beneficiary.

Residual private-law routes

What remains is a patchwork, none of it designed for the purpose. Negligence lies in principle but requires a duty of care in respect of data security, breach of the applicable standard, causation and quantifiable damage; there is little authority on the first, and the damage requirement reproduces every difficulty catalogued in Part II. Breach of confidence is available

where information was imparted in circumstances importing an obligation of confidence, but as *Warren* illustrates it is poorly adapted to negligent security failures, since the gravamen is an omission rather than an act.

The most practically significant route is the Consumer Protection Act 2019. Where the claimant is a consumer of a service, a breach may be pleaded as a deficiency in service,³² and the consumer can offer an inexpensive and relatively expeditious procedure. The limitation is definitional rather than doctrinal: the Act reaches only relationships that constitute a service for consideration, excluding employment data, government databases and much platform processing undertaken without direct payment. Alongside it sits sectoral regulation, of which the Reserve Bank's directions on unauthorised electronic banking transactions are the clearest example, limiting or zeroing customer liability where the loss arises from a deficiency on the bank's part and is reported promptly.³³ The framework is genuinely effective within its domain, and that is also its limit: it compensates for the transaction, not for the breach.

The Indian position can be summarised in a sentence that would be paradoxical in either of the other two jurisdictions. A claimant may have her breach claim heard without difficulty, may establish that a constitutionally protected interest has been violated, and may still have no cause of action under which anything can be awarded to her. The filter has simply moved. The United States removes claims before the merits; England removes them at proof and quantum; India admits them and then discovers there is nothing at the end.

VI. Where the Gate Sits: The Comparative Argument

The typology of Part II can now be mapped onto the three systems. The United States accepts pecuniary loss and, narrowly, imminent risk, but treats mitigation costs as self-inflicted, finds distress and loss of control insufficient without concrete harm, and rejects statutory violation as an injury in federal court. England accepts pecuniary loss, distress and well-founded fear of misuse, but not loss of control presumed across a class, nor infringement alone. India recognises loss of control as a constitutional interest but, against private fiduciaries, offers compensation for little beyond pecuniary loss, through consumer law and sectoral rules. In each case acceptance follows the account of the law's function set out in Part II: restoration of loss in the United States, a compensatory conception hemmed in by procedure in England, and public regulatory enforcement in India.

The preceding sections were organised jurisdiction by jurisdiction because the doctrinal vocabulary genuinely differs. Article III standing has no analogue in England or India, and the tort of misuse of private information has no analogue in Indian or American law. Read together,

however, they converge on a single structural move made three times in three registers: each system erects a filter upstream of the merits, and that filter does the work a straightforward damages inquiry would otherwise have to do.

What unites these devices is that each can be read as a response to the anxiety, Cardozo CJ named in *Ultramares Corp v Touche*, the fear of liability in an indeterminate amount for an indeterminate time to an indeterminate class.³⁴ A data breach is the paradigm case of that fear realised. A single security failure can generate millions of technically injured claimants, most of whom will suffer nothing more concrete than exposure, and a legal system that compensates exposure as such invites liability calibrated to the size of the database rather than the gravity of the wrong. Article III standing, the positive-act requirement in *Warren*, the individualised-proof requirement in *Lloyd* and the DPDP Act's regulatory-only remedy are four devices that, whatever their stated rationale, have the same effect: they prevent exposure-based liability from following automatically, and at scale, from a single infrastructural lapse.

What should strike a comparativist is that this convergence occurs without borrowing. American courts reach it through Article III and the separation of powers; English courts through the internal architecture of tort and equity and the same-interest requirement; India through legislative choice. This is convergent evolution, not diffusion, and it supports the thesis pressed here: the difficulty is a structural feature of breach harm, namely its latency, its probabilistic character and its class-wide uniformity, which any mature legal system must contain by some mechanism, whatever vocabulary it speaks. The systems diverge on where the filter sits; they converge on why it exists.

The comparison also exposes a question each jurisdiction answers differently, and must answer differently given its constitutional structure: which institution is entrusted with deciding that mere exposure does not suffice for redress? In the United States it is a constitutional court policing the outer boundary of its own judicial power, an answer made possible only by the case-or-controversy requirement. The restriction is therefore jurisdictional rather than substantive. Congress may not simply legislate around *TransUnion* by declaring a harm concrete, but a state legislature or state court, operating outside Article III, may reach a different result on identical facts, as *Rosenbach* shows. The gatekeeping function is deliberately fragmented between federal and state fora.

In England the decision-maker is a common law court policing the boundaries of its own remedial categories, an internal and doctrinal form of gatekeeping exercised through precedent, the strike-out and summary judgment jurisdiction, and the interpretation of the representative action rule. Parliament remains sovereign and could legislate a different regime; its silence

leaves room for continued judicial recalibration, as *Farley* shows. In India the decision-maker is the legislature, and it has made an unusually candid institutional choice: that regulatory deterrence, not private compensation, is the appropriate response to data harm short of quantifiable loss. This is not a court declining jurisdiction or refusing to extend a remedy, since the Indian judiciary has if anything been more willing than its counterparts to recognise the underlying interest as a fundamental right. The gate is erected by Parliament after the constitutional right has been recognised, which produces the paradox already flagged: the interest is elevated to constitutional status in the very years preceding a statute that declines to let an individual sue on it.

VII. Risk, Causation and Time

A data breach does not itself defraud anyone. It creates a pool of exposed information that a third party, usually unidentified and often never apprehended, may or may not later exploit. The injury, if it comes, comes later and through an intervening criminal act for which the breached defendant is not directly responsible. This temporal structure makes breach litigation different in kind from a car accident or a defective product: the defendant's wrong is complete at the moment of the breach, but the claimant's injury lies in the future and depends on the independent choice of a stranger. American courts made the feature doctrinally explicit through the certainly impending standard of *Clapper*, whose speculative chain of possibilities runs from breach, to use or sale by the thief, to selection of this claimant's data, to successful fraud.

Tort's traditional architecture assumes a completed, individuated injury: the claimant was hurt, the defendant caused it, damages compensate the loss. Breach harm does not fit, because for the great majority of claimants nothing has happened except an increase in the probability that something will. The closest pre-digital analogue is toxic exposure, and the comparison is instructive because American courts resisted compensating bare exposure there too. In *Metro-North Commuter Railroad Co v Buckley* the Supreme Court held that a railway worker exposed to asbestos dust, facing a statistically real but unrealised increase in cancer risk and showing no symptoms, could not recover medical monitoring costs absent a present physical injury, reasoning that recovery for exposure alone would generate a flood of claims from the worried well.³⁵ California reached the opposite conclusion on broadly similar facts in *Potter v Firestone Tire & Rubber Co*, allowing monitoring costs where expert evidence showed future surveillance to be a reasonably certain consequence of exposure.³⁶ The two decisions reach opposite results because federal and state courts weigh the indeterminate-liability concern differently, which is exactly the fracture line running through the breach cases that followed.

Even a claimant who clears the threshold confronts a second, independent problem once her data has been misused. By the time fraud occurs her information may have passed through several breaches, several brokers and several criminal resales, so that no single defendant's conduct can be shown on the ordinary but-for or substantial-factor standard to have caused the harm. The Seventh Circuit met this directly in *Remijas*, where the defendant argued that other contemporaneous retail breaches severed the causal link; the court held that the existence of other breaches had no bearing on traceability for standing purposes, but was careful to note that this was a threshold ruling and to leave causal attribution for trial. That deferral is telling: aggregation does not disappear once standing is granted, it resurfaces at causation, where the tools of tort law were built for a single tortfeasor and a single accident. India offers a real-world illustration. In October 2016 malware compromised a payment switch provider, exposing roughly 3.2 million debit cards across several large banks at once;³⁷ a customer defrauded afterwards could not principally attribute her loss to her own bank rather than to the switch provider or the card networks.

All three systems reproduce a version of the same bind for the claimant who tries to act responsibly in the interval between breach and possible fraud. If she does nothing and fraud never materialises, she has no injury to plead. If she buys credit monitoring, freezes her file or spends hours reviewing statements, American courts have frequently told her these are self-inflicted costs that cannot manufacture standing, which is *Clapper's* reasoning extended by analogy. Yet if she does nothing and is later defrauded, the delay between notice and injury becomes an argument that the harm was foreseeable and avoidable, inviting a plea of contributory fault. Prudence looks like manufactured injury; imprudence looks like contributory negligence. England's version operates through quantum: after *Rolfe* a claimant who spent money or anguish over a trivial breach risked being told her response was disproportionate, a risk *Farley* eases but does not remove.

The acceptance in *VB* that well-founded fear of future misuse can itself be non-material damage looks like a way out. If fear is the damage, the claimant need not wait for the criminal act that *Clapper* treats as a precondition, and she need not solve the aggregation problem, since her fear is traceable to the one breach she can identify. *Farley* has brought the same position into English law. But the Court of Justice cabined the holding in a way that limits how much weight it can bear: the fear must be well founded in the specific circumstances, a question the national court must verify rather than presume, and the claimant still carries the burden of proving she personally experienced it. This does not eliminate the evidentiary problem. It relocates it from a question about the external world, whether this data will be misused, to a question about the

claimant's internal state, whether she genuinely and reasonably feared that it would be, trading one hard-to-verify fact for another.

VIII. Aggregation and the Individualised-Harm Requirement

A data breach produces an almost pure specimen of the negative value suit: millions of claims, each worth individually far less than the cost of litigating it. No sensible claimant spends money suing over a stolen card number that costs forty minutes and a phone call to resolve, and no lawyer takes the case on a contingency calculated against that sum. The economic logic of pursuing the claim depends entirely on aggregation, on turning a million worthless suits into one suit worth pursuing. Posner J captured the point in *Carnegie v Household International Inc*: the realistic alternative to a class action is not seventeen million individual suits but zero.³⁸ The Supreme Court had made the same structural observation in *Amchem Products Inc v Windsor*, recognising that Rule 23(b)(3) exists precisely to vindicate claims that would otherwise go unlitigated.³⁹

But the feature that makes aggregation necessary sits in tension with the doctrinal precondition for it: that the claims share a common harm capable of class-wide proof. A breach exposes a uniform category of data to a uniform category of risk, which looks like exactly the kind of common question collective procedure was built to resolve. The difficulty is that the law in all three jurisdictions refuses to treat exposure itself as the compensable event, insisting instead on individualised proof of fraud, distress or concrete consequence. Individual claimants cannot afford to prove that individually; a class cannot be certified to prove it collectively, because individualised proof is by definition not common. The size of the class that shares the claim is simultaneously the reason she needs a class action and the reason she cannot get one certified. *TransUnion* is, on its procedural facts, a certification case as much as a standing case, and that dual character is what makes it decisive here. The case had gone to a jury verdict for a certified class, and the Court held that Article III standing must be shown for every class member seeking damages. The lesson for subsequent breach litigation is clear in direction, though not in every detail: a class that lumps together members who can show concrete harm with members who cannot is likely to fail at the threshold, because sorting them is an individualised inquiry that may defeat predominance before trial. District courts have had to engineer classes around the constraint, narrowing definitions to members whose data was actually misused or splitting subclasses by category of harm. The no-injury class, in which counsel could certify broadly and let damages sort themselves out later, is now difficult to sustain in federal court, although whether uninjured members may remain in a certified class is still contested.

England arrived at a structurally identical result through a different vehicle. *Lloyd* tried to use the representative action, the nearest thing English procedure has to an opt-out class, to litigate a uniform per capita loss-of-control claim. Its rejection confirmed what the Court of Appeal had held a decade earlier in *Emerald Supplies Ltd v British Airways plc*: a representative action requires every represented person to share the same interest at every stage, not merely at judgment, and that requirement collapses the instant individualised proof of loss becomes necessary.⁴⁰ The gap this leaves is structural rather than incidental. England does possess a genuine opt-out collective regime, introduced for competition claims and litigated before the Competition Appeal Tribunal,⁴¹ but it is confined to antitrust harm, where loss can often be modelled economically across a class. No equivalent opt-out regime exists for data protection. Section 187 of the Data Protection Act 2018 allows a representative body to bring a claim for data subjects who have authorised it, but only on an opt-in basis, because the opt-out power in Article 80(2) GDPR has not been enacted. Otherwise, the breach claimant is left with the opt-in Group Litigation Order. Both require claimants to come forward individually and so reintroduce exactly the negative-value problem.

India presents the starkest version, because its collective tools were built for other problems. Section 35(1)(c) of the Consumer Protection Act 2019 permits a complaint by one or more consumers where there are numerous consumers having the same interest,⁴² and the Supreme Court in *Brigade Enterprises Ltd v Anil Kumar Virmani* confirms that the consumer fora apply a same-interest test strikingly similar to the English standard.⁴³ A representative consumer complaint over a breach would therefore face the identical individualised-proof obstacle that sank *Lloyd*, the moment claimants' circumstances diverge. Public interest litigation, the device that gave India its permissive standing doctrine, does not fill the gap, because it is directed chiefly at public wrongs and public bodies and cannot reach a private data fiduciary.

Read together, these three failures support a conclusion more precise than hostility to breach claims. The individualised-harm requirement rarely defeats a single well-evidenced claim outright: a claimant who can show an actual fraudulent charge, a diagnosable anxiety disorder or a well-founded fear generally has some route to a remedy in all three systems, however narrow. What the requirement reliably defeats are aggregation, because the moment a class needs individualised proof to establish membership it stops being a class. The injury requirement's deepest effect is not substantive but structural: it decides not so much who wins as how many people can sue together, and in doing so it decides whether private litigation can do any deterrent work at all.

IX. Rethinking the Compensable Injury

One way out of the dilemma is to stop asking whether a breach caused measurable loss and ask instead whether it violated a right, on the model of torts that have never required proof of damage. English law has long recognised torts actionable per se: trespass to land, battery and libel are wrongs for which a claimant recovers absent any provable financial or physical consequence, because the wrong lies in the violation of the right itself. Varuhas has given this structure its fullest treatment, arguing that such torts serve a vindictory function distinct from compensation, with damages awarded for the normative loss of having one's right infringed, assessed objectively and without regard to consequential effects.⁴⁴

Recasting a breach as this kind of wrong is intuitively appealing, since the right to control personal information is violated the moment the information is exposed, so a conventional award could vindicate the right without proof of probabilistic, aggregation-resistant harm. But the proposal meets a live doctrinal headwind within the tradition it borrows from. The High Court of Australia in *Lewis v Australian Capital Territory* rejected a freestanding head of vindictory damages even for false imprisonment, holding that nominal damages and a declaration sufficed where no measurable harm was shown, and that courts should not invent a larger damages category simply to mark disapproval.⁴⁵ If common law courts are reluctant to extend substantial vindictory awards within torts that have recognised the model for centuries, importing it wholesale into a statutory field is harder still. A legislature is the more realistic vehicle, which points back to statutory damages.

Solove and Citron take a different route to the same destination. Rather than bypassing harm, they argue that courts have been too quick to dismiss risk and anxiety as non-cognisable when other fields of American law, including environmental exposure and medical monitoring, already compensate probabilistic and psychological injury using disciplined evidentiary standards.⁴⁶ Calo, responding in the same journal, largely agrees with them but suggests the analysis is missing a step: whether Congress can create a protectable interest in freedom from privacy risk or anxiety, or whether the nature of such injuries itself offends Article III.⁴⁷ That is the question *TransUnion* has since answered restrictively (Part III). It also leaves open an objection this article presses on its own account, one descended from Cardozo's: a standard that lets any exposed data subject plead compensable anxiety invites uncapped, scale-indifferent liability. A disciplined evidentiary standard applied at the scale of a national credit-bureau breach still produces tens of millions of individual psychological assessments, an evidentiary problem different in degree but not obviously in kind from the aggregation failure already

described.

If courts are institutionally reluctant to price risk and anxiety, the legislature can set the price in advance, which is what Illinois did with BIPA and California with the CCPA. BIPA provides liquidated damages without proof of injury;⁴⁸ the CCPA confines its breach action to specified sensitive data and fixes damages within a per-consumer, per-incident range.⁴⁹ Both solve by fiat every problem surveyed here: no standing inquiry, no causation puzzle, no individualised proof, and no aggregation obstacle, since a class defined by a uniform statutory entitlement is the paradigm case collective procedure was built for. The cost showed up in *Cothron v White Castle System Inc*, where the Illinois Supreme Court held that a separate violation, and therefore a separate award, accrues each time biometric data is scanned or transmitted rather than on first collection.⁵⁰ The lesson is double-edged. A flat per-violation sum removes every evidentiary and procedural obstacle, but divorced from any scaling to severity or sensitivity it generates liability disconnected from any plausible measure of harm. The CCPA's narrower, category-limited design is an implicit first attempt at sensitivity-based tiering.

A more calibrated middle path would key the size of a presumptive award to the sensitivity of the data breached, with biometric and health data at the top, financial credentials in the middle and contact information lower, combining BIPA's simplicity with the CCPA's scoping while capping recovery per breach event rather than per discrete transaction. A second option is a presumptive minimum triggered by defined categories of breach, such as unencrypted sensitive data exfiltrated by a confirmed external attacker, rebuttable by the defendant but otherwise payable on proof of membership in the breached class.

The third hybrid, a compensation fund financed from regulatory penalties, is the most natural graft onto the DPDP Act, precisely because that architecture already does the hard institutional work of collecting the penalty; what it lacks is a pipe connecting the penalty to the injured data principal. India has a partial precedent in the Securities and Exchange Board of India's Investor Protection and Education Fund, which has occasionally been used to make restitution to harmed investors, unlike most penalties, which go to the Consolidated Fund.⁵¹ A DPDP fund built on that template would need to avoid the precedent's defects: an express statutory entitlement to a share of collected penalties rather than a discretionary utilisation power, a presumptive rather than individually litigated causal link between breach and membership in the affected class, and a defined disbursement mechanism rather than reliance on the Board's unstructured discretion.

The institutional map determines how much of this menu each jurisdiction can adopt. A federal American statutory-damages regime would still have to clear *TransUnion*'s constitutional floor,

since Congress cannot declare a harm concrete, unless it created state-law rights enforceable in state court. England's path runs through Parliament: nothing in *Lloyd*, *Warren* or *Farley* forecloses a statutory minimum, and *VB* and *Farley* already supply a template for compensating well-founded fear. India's position is the inverse, because the obstacle has never been doctrinal. Parliament, having built the DPDP Act's penalty architecture around regulatory deterrence, has simply not taken the one further step of directing a defined share of that revenue to the people it was meant to protect.

X. Conclusion

Data breach litigation exposes a gap between what the law can recognise and what it can price. A claimant whose data has been exposed but not misused has suffered something real, but it is latent, probabilistic and uniform across a class. This article has argued that the three jurisdictions respond with filters placed at different stages. The United States filters at the threshold, through Article III standing. England filters at proof and procedure, through individual proof, the closing of the equitable routes and the limits on representative actions. India filters at the remedy, through a statute that penalises fiduciaries without compensating data principals. The filters differ because the institutions differ, but they have the same effect: containing indeterminate liability.

The conclusions that follow are as stated. First, the injury requirement rarely defeats a well-evidenced individual claim; its deeper effect is on aggregation, because individualised proof is exactly what a class cannot supply. Whether private litigation can deter anything therefore depends on how collective claims are structured, not only on how injury is defined. Second, the reforms that work around the problem, including statutory damages, sensitivity-tiered presumptive awards and compensation funds, are legislative, and each jurisdiction's institutional position determines which are available. Third, if the compensable harm is to be located, it lies on this article's account not in exposure as such but in objectively well-founded fear of misuse, supplemented by legislatively set presumptive sums for defined categories of breach where individual proof is uneconomic. For India, the most natural step is also the smallest: directing a defined share of DPDP penalties to the individuals whose data was exposed.

References

1. The Constitution of the United States of America, 1787 art III.
2. *Clapper v Amnesty International USA* 568 US 398 (2013) 410, 416.
3. *Spokeo Inc v Robins* 578 US 330 (2016) 340-41.
4. *TransUnion LLC v Ramirez* 594 US 413 (2021) 417, 439-40.
5. *Remijas v Neiman Marcus Group LLC* 794 F 3d 688 (7th Cir 2015) 693.
6. *Galaria v Nationwide Mutual Insurance Co* 663 F App'x 384 (6th Cir 2016) 388.
7. *Reilly v Ceridian Corp* 664 F 3d 38 (3d Cir 2011) 43.
8. *Beck v McDonald* 848 F 3d 262 (4th Cir 2017) 275.
9. *In re SuperValu Inc* 870 F 3d 763 (8th Cir 2017) 771.
10. *Rosenbach v Six Flags Entertainment Corp* 2019 IL 123186, 129 NE 3d 1197 (Ill 2019) [33]-[34].
11. *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003 [43], [105].
12. The Data Protection Act 1998, s 13(2).
13. *Lloyd v Google LLC* [2021] UKSC 50, [2022] AC 1217 [115]-[139].
14. The Civil Procedure Rules 1998, SI 1998/3132, r 19.8 (formerly r 19.6).
15. *Rolfe v Veale Wasbrough Vizards LLP* [2021] EWHC 2809 (QB), [2022] EMLR 6 [38]-[43].
16. *Johnson v Eastlight Community Homes Ltd* [2021] EWHC 3069 (QB) [1], [27]-[29].
17. *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB), [2021] EMLR 25 [26]-[28].
18. The Data Protection Act 2018; Regulation (EU) 2016/679 as retained in United Kingdom law (UK GDPR) art 82.
19. Case C-300/21 *UI v Österreichische Post AG* ECLI:EU:C:2023:370 [42], [51].
20. Case C-340/21 *VB v Natsionalna agentsia za prihodite* ECLI:EU:C:2023:986 [85]-[86].
21. *Farley v Paymaster (1836) Ltd* [2025] EWCA Civ 1117.
22. *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 [297], [325]; The Constitution of India, 1950 arts 12 and 21.
23. *Rudul Sah v State of Bihar* (1983) 4 SCC 141, 147; The Constitution of India, 1950 arts 32 and 226.
24. The Information Technology Act, 2000 (21 of 2000) s 43A.
25. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) r 3, r 8.
26. The Digital Personal Data Protection Act, 2023 (22 of 2023) s 44(2).
27. *ibid* ss 27 and 33, Sch.
28. *ibid* s 34.

29. *ibid* ss 11-14 and s 15.
30. Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology 2018) cl 75.
31. The Personal Data Protection Bill, 2019 (Bill No 373 of 2019) cl 64.
32. The Consumer Protection Act, 2019 (35 of 2019) s 2(11) and s 2(42).
33. Reserve Bank of India, 'Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' (6 July 2017) DBR.No.Leg.BC.78/09.07.005/2017-18.
34. *Ultramares Corp v Touche* 174 NE 441 (NY 1931) 444 (Cardozo CJ).
35. *Metro-North Commuter Railroad Co v Buckley* 521 US 424 (1997) 442-44.
36. *Potter v Firestone Tire & Rubber Co* 863 P 2d 795 (Cal 1993) 823-25.
37. 'Debit Card Data Breach: 32 Lakh Cards Compromised' *The Economic Times* (Mumbai, 20 October 2016).
38. *Carnegie v Household International Inc* 376 F 3d 656 (7th Cir 2004) 661 (Posner J).
39. *Amchem Products Inc v Windsor* 521 US 591 (1997) 617; Federal Rules of Civil Procedure, r 23(b)(3).
40. *Emerald Supplies Ltd v British Airways plc* [2010] EWCA Civ 1284, [2011] Ch 345 [62]-[65].
41. The Competition Act 1998, ss 47A-47B, as amended by the Consumer Rights Act 2015, s 81 and Sch 8.
42. The Consumer Protection Act, 2019 (35 of 2019) s 35(1)(c).
43. *Brigade Enterprises Ltd v Anil Kumar Virmani* (2022) 4 SCC 138 [17]-[20].
44. Jason NE Varuhas, *Damages and Human Rights* (Hart Publishing 2016) 46-53.
45. *Lewis v Australian Capital Territory* [2020] HCA 26, (2020) 271 CLR 192 [26]-[31].
46. Daniel J Solove and Danielle Keats Citron, 'Risk and Anxiety: A Theory of Data-Breach Harms' (2018) 96(4) *Texas Law Review* 737, 756-62.
47. Ryan Calo, 'A Long-Standing Debate' (2018) 96 *Texas Law Review Online* 59, 61-64.
48. The Biometric Information Privacy Act 2008, 740 ILCS 14/20(1)-(2).
49. California Civil Code, s 1798.150(a)(1).
50. *Cothron v White Castle System Inc* 2023 IL 128004 [23]-[30].
51. The Securities and Exchange Board of India Act, 1992 (15 of 1992) s 11 and s 15JA.