Singapore Journal of Legal Studies
[2026] 11–45

THE SURPRISING VIRTUES OF HETEROGENEITY: LEGAL PLURALISM AND THE GOVERNANCE OF GENERATIVE AI

Daryl **Lim***

This Article argues that the United States' fragmented approach to generative AI regulation is a strategic strength rather than a flaw. In place of a single federal regime, privacy law, the right of publicity, and copyright offer overlapping tools to address identity-linked harms, each grounded in distinct theories of harm and institutional traditions. This pluralism promotes experimentation, learning, and well-reasoned development rather than confusion. Heterogeneous governance helps courts and lawmakers adapt incrementally to fast-moving technologies, avoid premature lock-in, and coordinate protections across legal silos. To build on these advantages, the Article proposes a narrowly tailored data right focused on high-fidelity, identity-linked uses of data. Functioning as an opt-in, transparency-driven supplement to existing doctrines, this right would close gaps while preserving innovation and doctrinal diversity. The result is a principled, pragmatic approach that safeguards individual agency and leverages the adaptive strengths of US federalism.

I. Introduction

Generative AI collapses boundaries that once separated identity, creativity, and data. A single deepfake of Taylor Swift can implicate privacy interests, violate publicity rights, raise copyright questions, and trigger First Amendment concerns.[1] As these technologies increasingly ingest, remix, and monetize identity-linked data, the legal system faces a pressing question: What tools can safeguard individual agency over the digital self? Privacy torts respond to dignitary harm, the right of publicity addresses commercial misappropriation, and copyright protects expression.[2]

---

* H. Laddie Montague Jr. Chair in Law; Associate Dean for Research and Strategic Partnerships; Founding Director, Intellectual Property Law and Innovation Initiative; Co-hire, Institute for Computational and Data Sciences and Affiliate, Center for Socially Responsible Artificial Intelligence, Penn State University. Academic Fellow, National University of Singapore Centre for Technology, Robotics, Artificial Intelligence & the Law (TRAIL). This working paper was written for the "IP & Technology in the 21st Century Conference: Challenges in the Next Decade" conference at the National University of Singapore. I am grateful to David Tan for his invitation to contribute this article, as well as to Sandra Annette Booysen, Mark McBride, and their team at the Singapore Journal of Legal Studies for their thoughtful editorial guidance and exemplary professionalism throughout the publication process.

1 Kevin Frazier, "Swift Justice? Assessing Taylor's Legal Options in Wake of AI-Generated Images" (2024), Tech Policy Press, <https://www.techpolicy.press/swift-justice-assessing-taylors-legal-options-in-wake-of-aigenerated-images/>. See also generally, David Tan, *The Commercial Appropriation of Fame: A Cultural Analysis of the Right of Publicity*, (Cambridge University Press, 2017) (Illustrating how a practical framework that accounts for how fame is produced, shared, and consumed can enhance our understanding of the legal protections surrounding the commercial value of celebrity identity).

2 *Infra* Part III.

Yet none of these frameworks fully captures the extraction and transformation of personal data when outputs defy conventional categories. For example, an AI-generated song that mimics Taylor Swift's vocal timbre and lyrical style, without copying existing lyrics or recordings, may not infringe copyright. However, it evokes her identity in ways that feel exploitative. It borrows her voice (a property interest protected by the right of publicity), constructs lyrics in her persona (a creative output), and deploys these for public consumption and monetization, all without her consent. This kind of synthetic output blurs legal boundaries, exploiting the expressive and commercial value of identity while evading the doctrinal triggers that existing laws rely on.

Ideologically, American political culture remains sceptical of centralized regulatory solutions.[3] Other jurisdictions have embraced more centralized or coordinated strategies to govern generative AI and its associated risks. For instance, unlike the European Union or China, the United States (US) has a much less unified regulatory strategy.[4] Nor is one likely to emerge in the near term. Policymakers are often reluctant to constrain innovation, particularly when national competitiveness is framed as a priority.[5]

The Trump AI Action Plan's emphasis on national competitiveness echoes broader geopolitical anxieties surrounding AI.[6] While affirming democratic values and federalism, the plan's top-down approach reflects an emerging federal desire to consolidate disparate initiatives under a common national purpose. Whether this approach will supplement or supplant the pluralist experimentation already underway across states and legal doctrines remains to be seen. Its release underscores the growing need to establish regulatory coherence without compromising legal heterogeneity.

The US relies on a patchwork of sector-specific statutes, evolving common law doctrines, and soft law instruments.[7] Institutionally, American lawmaking is fragmented by constitutional design.[8] Congress acts slowly, particularly in domains

---

3 John W Kingdon, *America The Unusual* (Palgrave Macmillan, 1999) ("As a general rule, Americans think that government should be much more limited than citizens of other countries do.").

4 *Infra* Part V. See also Matthew Sag & Peter K. Yu, "The Globalization of Copyright Exceptions for AI Training" (2025),74 Emory LJ 1163.

5 "Transcript: The Futurist: America's Technological Edge", *Washington Post Live* (March 25, 2025) (remarks of Rep. Brett Guthrie) (Rep. Brett Guthrie emphasized that the U.S. must "beat China" in Al leadership, warning against over regulation like in Europe and underscoring that "[t]here are people in town that think you should regulate like Europe or California regulates, and I think that puts us in a position where we're not competitive."). President Trump made a similar remark regarding fair use in July. See *infra* note 102.

6 The White House, *America's AI Acton Plan*, (July 2025), <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf> [The White House]. See also Barry Pavel et al., "AI and Geopolitics: How Might AI Affect the Rise and Fall of Nations?" (2023), Rand Corp., Persp. Paper PEA 3034-1, <https://www.rand.org/pubs/perspectives/PEA3034-1.html> ("Nations across the globe could see their power rise or fall depending on how they harness and manage the development of artificial intelligence (AI).").

7 *Infra* Part III.

8 *Infra* Part II. See also Sean Farhang & Miranda Yaver, "Divided Government and the Fragmentation of American Law"(2016), 60 American Journal of Political Science 401 at 501, <https://www.jstor.org/stable/24877629> (describing the "fragmented and decentralized American style of policy implementation.").

where technology outpaces deliberation.[9] A recent bipartisan proposal, the No AI FRAUD Act, introduced by Senators Hawley and Blumenthal, illustrates both the promise and limitations of federal intervention.[10] The bill would create a private right of action allowing individuals to sue AI companies and platforms that misappropriate their creative works or likeness without consent.[11] While still at the proposal stage, it reflects growing legislative interest in safeguarding individual identity and expression against generative AI misuse.[12] Its emergence signals a tentative step toward harmonisation, yet its narrow scope and uncertain trajectory underscore why more agile, pluralist mechanisms remain necessary in the near term.

Similarly, recent legislative attention, including hearings before the U.S. Senate Judiciary Subcommittee on Intellectual Property, suggests a growing interest in establishing a federal right of publicity.[13] Universal Music Group, Adobe, Stability AI, and other industry stakeholders have called for statutory clarity to address unauthorised commercial use of publicity rights in generative AI outputs.[14]

A narrowly tailored data right offers a constructive response. The goal is not to replace existing doctrines, but to reinforce them. The data right draws from the autonomy interests protected by privacy law, the dignity values embedded in publicity doctrine, and the incentive structures central to copyright. Its central premise is that individuals should retain meaningful input into how their identities are co-opted for technological and economic purposes.

Such a right would empower individuals to control how their voice, likeness, biometric patterns, and even expressive style are used in AI training and deployment.[15] It offers individuals a clear, affirmative entitlement, regardless of whether such data is protected under existing frameworks. This right would not replace existing regimes but would complement them by filling doctrinal blind spots, especially in cases where personal data is used non-consensually yet eludes traditional categorisation. In doing so, it preserves the benefits of legal pluralism while reducing fragmentation and ensuring more consistent redress for emerging harms driven by AI.

Importantly, the right would apply with precision. It would target sensitive uses, such as synthetic identity generation, emotion simulation, or high-fidelity

---

9 Perkins Coie LLP, "States Begin to Regulate AI in Absence of Federal Legislation", Perkins Coie (May 22, 2024), <https://perkinscoie.com/insights/update/states-begin-regulate-ai-absence-federal-legislation>. ("[T]he U.S. Congress has made noise about the need for federal AI legislation, but progress has been slow.") See also Maya Kornberg, Marci Harris & Aubrey Wilson, "Congress Must Keep Pace with AI" (2024), Brennan Centre for Justice, <https://www.brennancenter.org/our-work/research-reports/congress-must-keep-pace-ai>.

10 H.R. 6943, No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act of 2024, 118th Cong, 2024) (United States). See also Josh Hawley & Richard Blumenthal, *Hawley, Blumenthal Unveil Bipartisan Bill Empowering Working Americans to Sue Big Tech, AI Companies for Stealing Creative Works*, U.S. Senate (July 21, 2025), <https://www.hawley.senate.gov/hawley-blumenthal-unveil-bipartisan-bill-empowering-working-americans-to-sue-big-tech-ai-companies-for-stealing-creative-works>.

11 *Ibid*.

12 *Infra* Part IIIB.

13 Steve Brachmann, "Senate IP Subcommittee Mulls Federal Right of Publicity at AI and Copyright Hearing", *IPWatchdog* (July 13, 2023), <https://ipwatchdog.com/2023/07/13/senate-ip-subcommittee-mulls-federal-right-publicity-ai-copyright-hearing>.

14 *Ibid*.

15 *Infra* Part IV.

replication. It would not obstruct AI development more broadly, nor would it grant blanket control over publicly available data. Instead, it would function as a scalpel, offering narrowly tailored rules that protect the most personal dimensions of identity without impeding legitimate innovation.

This calibrated approach aligns with the principles outlined in President Trump's AI executive order, which emphasised both safeguarding American values and accelerating innovation.[16] While harmonisation may offer baseline protections, the persistence of heterogeneity at the state level, such as divergent recognition of postmortem rights or the inclusion of voice and gesture, offers a valuable sandbox for innovation and adaptation as AI capabilities evolve.[17] Rather than flatten these differences, policymakers might look to preserve diversity while ensuring minimum rights protections. By focusing on high-risk identity uses without overregulating the broader AI ecosystem, the proposed right advances that dual mandate.

The discussion proceeds as follows. Part II defends legal pluralism as a form of regulatory design. Part III examines how privacy, publicity, and copyright law address identity-linked harm and where they fall short. Part IV proposes a data right that operates as a harmonising layer rather than a replacement. Part V concludes.

II. Legal Pluralism as Regulatory Strategy

Legal pluralism, in its most basic sense, describes a landscape in which multiple, partially overlapping legal sources govern the same conduct.[18] In the United States, that landscape includes federal and state constitutions, statutes, common-law doctrines, agency regulations, industry self-regulation, and even private contracting norms.[19] Although this patchwork may seem like doctrinal clutter, the coexistence of many rules can foster experimentation, allowing doctrines to evolve through dialogue and competition. For AI, a technology whose affordances evolve faster than any single legislature can track, these dialogic pressures supply the feedback loop and adaptive governance that unitary codes lack.

Before proceeding, it is useful to distinguish between federalism and legal pluralism, which are related but analytically distinct. Federalism refers to the constitutional allocation of authority between national and subnational governments—. In the US, this means the division of power between the federal and state governments.[20] Legal pluralism, by contrast, encompasses the coexistence of federal,

---

16 The White House, *supra* note 6. See also *Ibid*. at 12 – 13 (discussing deepfakes).

17 The recognition and scope of postmortem publicity rights differ significantly among states, creating a patchwork of legal standards. See *eg*, *Estate of Bisignano by and through Huntsman v. Exile Brewing Company, LLC*, 694 F.Supp.3d 1088 (2023) (protecting common law publicity rights postmortem in Iowa for as long as they are actively used, and even when they are not actively exploited at the time of death.). *cf*. *Shaw Family Archives Ltd. v. CMG Worldwide, Inc.*, 486 F.Supp.2d 309 (2007) (New York does not recognize any common law right of publicity and limits statutory publicity rights to living persons.).

18 Paul Schiff Berman, "From Legal Pluralism to Global Legal Pluralism" in Richard Nobles & David Schiff eds. *Law, Society and Community: Socio-Legal Essays in Honour of Roger Cotterrell* (Ashgate, 2014).

19 Barak Orbach, "What Is Regulation?" (2016) 30 Yale Journal on Regulation Online 1.

20 *Bond v. United States*, 564 U.S. 211, 221 – 222 (2011).

state, judicial, administrative, and private, that may overlap in governing the same conduct.[21] While federalism contributes to legal pluralism by enabling state-level innovation, pluralism also includes non-governmental norms, industry self-regulation, and hybrid enforcement structures.[22] This broader lens is especially relevant for generative AI, where legal governance emerges not only from traditional public law institutions but also from standards bodies, platform policies, and transnational frameworks. Recognising this distinction clarifies that the argument here is not a celebration of decentralisation per se, but an endorsement of regulatory diversity across both institutional and doctrinal domains.

Pluralism – and this is also relevant to other Commonwealth common law jurisdictions such as Singapore, Australia and India – enables courts, legislatures, and agencies to approach the same problem from different normative vantage points: privacy law from the perspective of autonomy, publicity from the perspective of dignity, and copyright from the perspective of incentives.[23] This convergence provides resilience; when one doctrine falters, another may offer a workable solution. For instance, consider the challenge of unauthorised use of a person's likeness by an AI-generated deepfake in a commercial advertisement. If a court finds that the right of publicity does not extend to synthetic depictions or is pre-empted by copyright, a plaintiff might instead bring a claim under privacy law for appropriation of identity.[24] Alternatively, if the deepfake incorporates expressive elements taken from a copyrighted work, such as a scene recreation from a movie, copyright law may provide a separate basis for relief, unless the elements are deemed to fall under, for example, the *scène à faire* doctrine, which excludes standard, non-original elements from copyright protection.[25] Each doctrine approaches and views harm differently, offering overlapping but distinct avenues of redress.

This doctrinal flexibility is mirrored in the institutional landscape, where legal innovation often emerges not from top-down mandates but from the gradual, decentralised efforts of courts and state legislatures. The iterative, bottom-up development of legal norms, exemplified by the privacy torts introduced by Warren and Brandeis in the 1890s and Illinois's Biometric Information Privacy Act (BIPA) in 2008, illustrates how subnational actors function as policy laboratories, experimenting with

---

21 William Twining, "Normative and Legal Pluralism: A Global Perspective" 20 Duke J Comp & Intl L 473 (2010) (Examining the relationship between legal pluralism, normative pluralism, and general normative theory from a global perspective.).

22 Erin Ryan, "Federalism as Legal Pluralism", in Paul Schiff Berman ed. *The Oxford Handbook of Global Legal Pluralism* (Oxford University Press, 2020) 482 ("Constitutional federalism, itself characterized by multiple sources of authority within a single geographical territory, provides a "vanilla" example of legal pluralism in action…").

23 *Infra* Part III.

24 In *re NCAA Student-Athlete Name & Likeness Licensing Litig.*, 724 F.3d 1268, 1271 (9th Cir., 2013). See also *Downing v. Abercrombie & Fitch*, 265 F.3d 994, 1003–1005 (9th Cir., 2001) (Discussing the boundary between copyright and right of publicity, holding that the latter is not preempted when based on the misappropriation of a persona); *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562, 573 (1977) (acknowledging the interplay between privacy rights and right of publicity, suggesting the availability of distinct causes of action depending on harm.).

25 *Eg, Warner Bros. Inc. v. American Broad. Cos.*, 720 F.2d 231, 240 (2d Cir., 1983).

rules that can be emulated or adapted by others.[26] Neither required Congress to overhaul federal privacy law. Instead, courts and state legislatures tested new rules on a smaller scale before their broader adoption. This iterative, bottom-up dynamic is difficult to achieve in unitary, code-centric systems, which must amend foundational instruments to keep pace.

In addition to adaptation, heterogeneity also encouraged doctrinal cross-pollination. California's Consumer Privacy Act (CCPA) borrowed opt-out and access concepts from the EU's General Data Protection Regulation (GDPR) but limited them to personal information.[27] Similarly, Tennessee's 2024 ELVIS Act then applied the CCPA's consent logic to the right of publicity, expressly targeting AI-generated voice and likeness.[28] Each move involved a different doctrinal toolkit, yet each drew inspiration from a neighbour's experiment, which is evidence that pluralism accelerates legal learning.

The federal NO FAKES Act extends this pattern of legal borrowing and synthesis.[29] While rooted in right of publicity doctrine, the legislation incorporates structural elements more commonly associated with privacy protection, such as consent requirements and notice provisions. The bill specifically targets unauthorised digital replication of a person's voice or likeness using AI, echoing Tennessee's ELVIS Act but broadening the intended scope to cover all individuals, not just performers. Its architecture, an intellectual property-like right blended with privacy principles, demonstrates how pluralistic legal ecosystems enable cross-domain borrowing to address novel technological harms.

Heterogeneity has its critics, key among them are uncertainty, forum shopping, and incoherence.[30] The convergence of multiple legal doctrines on the same identity-linked conduct is not without cost. Doctrinal overlap can expose developers and creators to duplicative liability, increase compliance complexity, and

---

[26] Ill. Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 et seq. (2008). See Anna L. Metzger, "The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy" (2019) 50 Loy U Chicago LJ 1051[Anna, "Litigation Rollercoaster"]

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [General Data Protection Regulation]. See Christian Auty, "Similarities and Differences Between the CCPA and GDPR" Logikcull Blog <https://www.logikcull.com/blog/similarities-and-differences-between-the-ccpa-and-gdpr>("I think it's fair to say CCPA borrowed some pretty core concepts from GDPR… the right to receive information about what a business has about you, the right to receive an actual copy of personal information, a right to deletion … Those are all concepts that we saw in GDPR and that were, I think, well-received …").

[28] Tennessee Code § 47-25-1101, 2024 (United States). See Sy Damle, Ivana Dukanovic, Britt Lovejoy & Alli Stilliman, "The ELVIS Act: Tennessee Shakes Up Its Right of Publicity Law and Takes on Generative AI", *Latham & Watkins Client Alert No. 3244* (Apr. 8, 2024) [Damle, Dukanovic, Lovejoy & Stilliman, "ELVIS Act"] (Expanding the state's statutory right of publicity by adding a cause of action not just for commercial use of an individual's voice or likeness but also against those who produce or distribute "an algorithm, software, tool, or other technology primarily intended to replicate a person's voice or likeness".).

[29] Nurture Originals, Foster Art, and Keep Entertainment Safe Act (No Fakes Act), S. 5680, 118th Cong., 2025 (United States).

[30] *Eg*, Samuel Issacharoff & Catherine M Sharkey, "Backdoor Federalization", (2006), 53 UCLA L Rev 1353 at 1388.

generate legal uncertainty about which standard governs.[31] Moreover, fragmentation can hinder accountability when doctrinal overlap creates uncertainty about which legal regime governs a particular harm, or when enforcement varies widely across jurisdictions. Fragmentation may also disadvantage individuals who lack the legal knowledge or resources to navigate multiple overlapping systems.[32] In areas such as transparency standards for training data, provenance documentation, or the auditability of AI models, a degree of harmonisation may not only be normatively desirable but also operationally necessary.

These apparent shortcomings can also be assets. Uncertainty creates space for doctrinal evolution and experimentation by avoiding premature lock-in to a single, possibly flawed, regulatory model. For that to happen, a clearer understanding of where these doctrines align, overlap, or conflict is essential for building a regulatory ecosystem that is both protective and predictable. Forum shopping can serve as a mechanism for litigants to expose underdeveloped doctrines or test new theories in sympathetic venues, thereby helping courts refine their boundaries through conflict and comparison. Apparent incoherence across jurisdictions may reflect productive pluralism rather than dysfunction, allowing legal systems to adapt to regional values, institutional competencies, and sector-specific needs. In aggregate, these features foster a dynamic regulatory environment that is better able to absorb shocks, learn from diverse experiments, and incrementally converge on more effective norms.

This dynamism is particularly evident in the interplay between litigation and legislation, where regulatory heterogeneity enables doctrinal cross-pollination. Litigation generates precedent that can be adopted or rejected elsewhere. Even overlapping mandates can coexist constructively, as seen with federal intellectual property laws that leave room for stronger state-level protections. For instance, the US Lanham Act's trademark provisions coexist with state unfair-competition laws.[33] A federal data right could replicate this strategy: establish baseline notice-and-consent duties for AI training while preserving space for states to craft stronger remedies tailored to local concerns, such as those in the entertainment or biometric industries. Illinois's emphasis on biometric privacy offers a useful template for how states can tailor protections to specific sectors, such as entertainment or healthcare. A federal baseline would provide uniform safeguards nationwide, while allowing states to tailor their responses to distinct local risks and industry practices.

Legal pluralism, then, is not an abdication of regulatory responsibility but a strategy of resilience. By tolerating friction, encouraging doctrinal borrowing, and maintaining multiple pathways for redress, the U.S. legal system is better equipped to confront the novel challenges posed by generative AI. Rather than striving for premature uniformity, policymakers should embrace the adaptive strengths that pluralism offers. This approach does not preclude eventual harmonisation but allows

---

[31] Julie E Cohen, "The Regulatory State in the Information Age", (2016), 17 Theor Inq L 369 at 386–388 (highlighting how fragmented regulatory frameworks can fail to constrain structural power in digital systems).

[32] See Daryl Lim, "Determinants of Socially Responsible AI Governance" (2025) 25 Duke L & Tech Rev 183 for how AI can promote access to justice.

[33] Mark P. McKenna, "Trademark Law's Faux Federalism" in Shyamkrishna Balganesh ed. *Intellectual Property and the Common Law* (Cambridge University Press, 2018) 288 at 288.

doctrines to mature in parallel, providing policymakers with a richer empirical and conceptual foundation for future reform.

III. Pluralism in Privacy, Publicity, and Copyright Law

The legal pluralism described in Part II becomes operational in the overlapping domains of privacy, publicity, and copyright. Each area of law responds to identity-linked harms in distinctive ways, but none alone is sufficient to address the multi-faceted challenges presented by generative AI.

For instance, while copyright protects original expression and privacy addresses non-consensual disclosures, the right of publicity uniquely targets the commodification of identity. Yet this doctrine struggles with deepfakes and digital clones that can simulate individuals' likenesses without any direct appropriation of copyrighted content or private facts.[34] Their interplay offers a composite framework that is more adaptable, context-sensitive, and resilient than any single doctrine acting in isolation.

A. *Information Privacy Law*

The American privacy tradition began not with comprehensive legislation, but with a theoretical call to action. Warren and Brandeis's 1890 article, "The Right to Privacy," proposed a common-law response to the intrusive technologies of their era, such as the camera and mass-print journalism.[35] That foundation later crystallised into Prosser's four privacy torts: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of name or likeness.[36]

These torts, while foundational, struggle to address the diffused, automated, and reputational harms that generative AI enables. For instance, imagine an AI-generated video that simulates a non-consensual speech by a private individual at a protest. Since the person is not a public figure and the video contains no actual footage or private facts, privacy torts may not be applicable. Yet the reputational fallout and emotional distress are substantial. Traditional tort requirements, such as proving individual damages or wrongful intent, are poorly suited for AI-generated content, which can be created and disseminated without direct human oversight.[37]

Moreover, the focus of privacy law on interpersonal wrongs does little to constrain institutional data harvesting or guide upstream practices. For example, litigation can force platforms to retain user data they had promised to delete, creating

---

[34] See *eg*, Samantha Nelson, "An AI Version of J.Lo Invites Travelers to Sail on Virgin Voyages", *Adweek* (July 7, 2023), <https://www.adweek.com/creativity/ai-j-lo-invites-travelers-to-virgin-voyages> (showing how AI-generated clones of celebrities such as "Jen AI," a licensed digital version of Jennifer Lopez used in a Virgin Voyages campaign blur the boundary between real and synthetic identities.).

[35] Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193.

[36] William Prosser, "Privacy", (1960), 48 Cal L Rev 383.

[37] Hannah R Sullivan & Scott J Schweikart, "Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?" (2019) American Medical Association Journal of Ethics at E101, <https://pubmed.ncbi.nlm.nih.gov/30794126/>.

conflicts between data minimisation principles and judicial discovery requirements.[38] Statutes like Illinois's BIPA offer a stronger template.[39] They shift emphasis from *ex post* remedies to *ex ante* compliance through opt-in consent and statutory damages.[40] However, BIPA's impact is geographically bounded, and its application depends on state recognition of biometric harms.

Pluralism, as explored in Part II, does not abandon legacy doctrines like privacy torts. Instead, it allows them to evolve, recombine, and borrow across domains. Privacy law contributes core normative principles, informational self-determination, consent, and proportionality, that are essential in building any coherent response to generative AI.[41] As discussed, these principles have influenced sector-specific laws like BIPA, which requires opt-in consent for the use of biometric identifiers, including voiceprints and facial geometry.[42]

As discussed further in Part IV, the proposed data right adopts privacy's most defensible and scalable principles, such as opt-in consent, access and deletion rights, and accountability, but recalibrates them for identity-linked AI applications. For example, rather than requiring a victim to prove reputational harm after the fact, the data right would allow individuals to pre-emptively control whether their voice or likeness may be used to train a generative model.[43] Moreover, by layering onto existing privacy statutes and common law, the data right avoids displacing pluralism. It harmonises disparate protections into a cohesive framework capable of responding to high-fidelity identity misuse while preserving space for innovation and speech.

This layered approach reflects pluralism's greatest strength: it permits overlapping regimes to address distinct aspects of the same harm. Privacy law alone cannot stop the creation of a viral deepfake. However, when paired with publicity doctrine (which focuses on commercial misappropriation) and copyright (which guards against appropriation of creative outputs), it becomes part of a more resilient and responsive system. The data right, in turn, operationalises this convergence. It codifies the privacy values embedded in BIPA, scales them nationally, and integrates them into a hybrid enforcement model that anticipates the unique challenges of generative AI.

---

38 *Eg, Victor Valley Union High School Dist. v. Superior Court*, 91 Cal.App.5th 1121 (2023).

39 Anna, "Litigation Rollercoaster", *supra* note 26.

40 Kirk J Nahra & Ali A Jessani, "Year in Review: 2023 BIPA Litigation Takeaways" WilmerHale Privacy & Cybersecurity Law Blog (Jan. 31, 2024); see also 740 Ill. Comp. Stat. 14/15 (United States) (requiring informed written consent prior to biometric data collection and providing for liquidated damages per violation).

41 *Eg, Pettus v. Cole*, 49 Cal.App.4th 402 (1996) (Recognising that informational privacy is central to the constitutional privacy provision and emphasising the need to maximise individual control over the dissemination and use of sensitive information to prevent unjustified embarrassment or indignity.); *Hill v. National Collegiate Athletic Assn*., 7 Cal.4th 1 (1994) (upholding the NCAA's drug testing program partly because it required advance notice and written consent from student-athletes, thereby respecting their autonomy and privacy expectations); *Lewis v. Superior Court*, 3 Cal.5th 561 (2017) (emphasising the importance of protective measures and safeguards to minimise privacy intrusions.).

42 740 Ill. Comp. Stat. Ann. 14/15(b) (United States) (mandating that private entities must obtain an individual's informed, written consent before collecting, capturing, purchasing, or otherwise obtaining their biometric data.).

43 *Infra* Part IV.

B. *The Right of Publicity*

The right of publicity, recognised in the state laws of over thirty US states, presently protects individuals against the unauthorised commercial exploitation of their name, image, voice, or other distinctive aspects of their identity.[44] Rooted in both dignity-based and property-based theories, the doctrine seeks to preserve personal autonomy while acknowledging the economic value of identity.[45] However, the rise of generative AI technologies capable of mimicking human likenesses, voices, and performances with unprecedented fidelity has pushed the doctrine to its conceptual and doctrinal limits.

Operating at the state level, the right of publicity remains unstable and fragmented, with significant variation across state laws – with significant variation in both statutory and common law protections – and no uniform federal standard.[46] While California's Civil Code § 3344 allows individuals to assert proprietary control over the commercial use of their name, image, or likeness, states like Maryland recognise only a common law appropriation tort; others, like New York and Illinois, impose differing thresholds for commercial exploitation and different duration for the recognition of such rights.

This state-by-state patchwork complicates enforcement, particularly in the context of generative AI, where likenesses and voices can be disseminated across platforms with national or global reach. The result is a regulatory vacuum that enables technological exploitation without clear accountability. These approaches risk severing the right from the person it is meant to protect, diluting its normative foundations, and undermining its role in safeguarding personal dignity in the digital age.

The advent of generative AI has vastly expanded the scope of potential misuse, with tools capable of mimicking voices, avatars, and performances.[47] A notable example arose in early 2023 when the song "Heart on My Sleeve," featuring AI-generated imitations of Drake and The Weeknd, went viral.[48] The song was

---

[44] *Bi-Rite Enterprises, Inc. v. Bruce Miner Poster Co., Inc*., 616 F. Supp. 71, 73 (1984) (""Right of publicity," when recognized, grants person exclusive right to control commercial value of his name and likeness and to prevent others from exploiting that value without permission.…"). See also *Midler v. Ford Motor Co*., 849 F2d 460, 463 (9th Cir., 1988) [*Midler*] ("A voice is as distinctive and personal as a face. The human voice is one of the most palpable ways identity is manifested. We are all aware that a friend is at once known by a few words on the phone. … The singer manifests herself in the song. To impersonate her voice is to pirate her identity.").

[45] In *re Hearst Commc'ns State Right of Publicity Statute Cases*, 632 F. Supp. 3d 616, 620 (S.D.N.Y., 2022) ("[T]he goal of maintaining a right of publicity is to protect the property interest that an individual gains and enjoys in his identity through his labor and effort."). See also, David Tan, *The Commercial Appropriation of Fame: A Cultural Analysis of the Right of Publicity*, (2017), Cambridge University Press 2017 45-62.

[46] David Atkinson & Jacob Morrison, *Unsettled Law: Time to Generate New Approaches*?, arXiv (July 2, 2024) (unpublished, archived at <arXiv:2407.01968>). ("While established legal frameworks, many originating from the pre-digital era, are currently employed in GenAI litigation, we question their adequacy.").

[47] Robert Booth, "AI Cloning of Celebrity Voices Outpacing the Law, Experts Warn", *The Guardian* (Nov. 19, 2024), <https://www.theguardian.com/technology/2024/nov/19/ai-cloning-of-celebrity-voices-outpacing-the-law-experts-warn>.

[48] Brian Hiatt, "Ready to Sing Elvis Karaoke . . . as Elvis? The Weird Rise of AI Music", *Rolling Stone* (June 28, 2023), <https://www.rollingstone.com/music/music-features/ai-music-drake-weeknd-ghostwriter977-beatles-elvis-voice-1234770094/>.

created by an anonymous producer known as Ghostwriter-977, and sparked legal and ethical debates around synthetic voice use in the music industry, a practice already familiar in film and gaming sectors, where digital replicas are used for dubbing or reshoots.[49]

Right of publicity claims involving voice frequently encounter copyright preemption defenses under the Copyright Act's broad scope.[50] This complicates enforcement, especially given recent U.S. Copyright Office guidelines limiting protection for AI-generated works.[51] In the case of Ghostwriter-977's track, it remains unclear what elements, if any, would qualify for copyright, raising uncertainty about whether the right of publicity can fill the regulatory gap. While federal preemption based on trademark law is less common, it occasionally arises where federal unfair competition doctrines intersect with publicity rights.[52] Still, publicity and trademark laws often operate in tandem to protect an individual's identity across various commercial contexts.

The right of publicity also sits uneasily with the First Amendment. The "transformative use" test, designed to safeguard expressive freedom in cases like *Comedy III Prods., Inc. v. Gary Saderup, Inc*., proves difficult to apply in AI contexts where outputs are novel but derivative.[53] Suppose an AI model generates a hyper-realistic, never-before-heard duet between a deceased singer and a contemporary artist. Is the resulting output transformative, derivative, or something in between? Courts must grapple with the fact that AI-generated works can be novel yet stylistically indistinguishable from the inputs on which they were trained. In such cases, the concept of transformative use may fail to guide the court to a principled legal resolution. A rebuttable presumption model, in which high-fidelity AI impersonations are presumed unlawful absent a compelling public interest, offers a more principled path.

If an AI-generated replica is indistinguishable from a real person's voice or likeness and deployed without consent, courts should presume infringement unless the user can demonstrate a strong public interest justification, such as satire, criticism, or documentary value, mirroring recognised categories of fair use under copyright law.[54] Such a framework maintains space for expressive freedom while creating

---

[49] *Eg*, Katrina Cabule, "Making AI Voices Ethical: Navigating Consent and Creativity in the AI Era", *Sonarworks Blog* (July 23, 2025) <https://www.sonarworks.com/blog/learn/ai-voice-ethics-consent-creativity>.

[50] 17 U.S.C. § 301(a) (United States). See *eg, Laws v. Sony Music Entertainment, Inc.*, 448 F.3d 1134 (2006) (Holding that a right of publicity claim based on the unauthorised duplication of a vocal performance contained within a copyrighted sound recording was preempted because the claim fell within the subject matter of copyright and asserted rights equivalent to those protected by the Act.).

[51] Eileen McDermott, "Copyright Office Makes AI Authorship Policy Official", *IPWatchdog* (Mar. 15, 2023), <https://ipwatchdog.com/2023/03/15/copyright-office-makes-ai-authorship-policy-official>.

[52] Jennifer E Rothman, "Navigating the Identity Thicket: Trademark's Lost Theory of Personality, the Right of Publicity, and Preemption" (2022) 135 Harv. L. Rev. 1271, 1337-38.

[53] *Comedy III Prods., Inc. v. Gary Saderup, Inc.*, 25 Cal.4th 387, 106 Cal.Rptr. 2d 126, 21 P.3d 797, at 804–808 (2001) (Importing "transformative" use from copyright law into the right of publicity context.). The test is widely adopted in a number of circuits. Eg, *Hart v. Electronic Arts, Inc.*, 717 F.3d 141 (3rd Cir., 2013); *Keller v. Electronic Arts, Inc*., 724 F.3d 1268 (9th Cir., 2013).

[54] Prithvi Iyer, "Transcript: U.S. Senate Judiciary Subcomm. on Intellectual Property Hearing on the NO FAKES Act", *Tech Policy Press* (May 1, 2024) ("[W]e made clear, long-recognized carve-outs, like, for example, parody and satire, remain available to creators to continue to foster the artistic and innovative potential of AI"), <https://techpolicy.press/transcript-us-senate-judiciary-subcommittee-hearing-on-the-no-fakes-act/>.

accountability for commercial or exploitative use of identity. Additionally, courts should consider adopting a tiered analysis that distinguishes between different functions of identity, such as artistic evocation, commercial endorsement, or reputational distortion. This more granular approach would align better with the complex and multi-functional uses of synthetic identity in AI contexts.

A recent decision from the Southern District of New York in *Lehrman & Sage v. Lovo, Inc.* further illustrates the doctrinal fault lines emerging in cases involving AI-generated identity clones.[55] Professional voice actors alleged that Lovo misused their recordings to train an AI voice synthesis model, producing clones marketed under different names for commercial use.[56] The court dismissed the copyright claims, holding that the Copyright Act protects only the fixed sound recordings, not the abstract qualities of voice or AI-generated imitations.[57] It also rejected Lanham Act claims for lack of false association or actionable consumer confusion.[58] However, it allowed the plaintiffs' breach of contract and right of publicity claims under New York Civil Rights Law to proceed.[59] Notably, the court emphasised that continued replication of the plaintiffs' voices through AI-generated outputs could constitute an ongoing violation, rejecting the defendant's narrow view of the statute of limitations.[60] The court also signalled a forward-looking interpretive approach, asserting that existing identity protections should be read to encompass evolving technologies like AI voice cloning.[61] This ruling underscores both the limitations of federal intellectual property law and the adaptive potential of state publicity statutes when confronted with novel forms of identity-based harm.

Public concern is no longer confined to celebrities; everyday individuals are vulnerable to reputational harm from AI-generated impersonations.[62] As mentioned in Part II, Tennessee's 2024 ELVIS Act reflects a legislative response, offering post-mortem rights and statutory damages for unauthorised AI-generated replicas.[63] By prioritising personal autonomy over commercial fame, the Act broadens the scope of protection to ordinary individuals, setting a potential model for federal reform. The federal NO FAKES Act, builds on this momentum by proposing a nationwide "digital replica right."[64] While rooted in the logic of the right of publicity, the bill borrows procedural elements from privacy and consumer protection law, such as consent requirements and state enforcement, signalling a hybrid regulatory approach

---

55 *Lehrman v. Lovo, Inc.*, No. 24-CV-3770 (JPO) (S.D.N.Y., July 10, 2025).

56 *Ibid*. at *1.

57 *Ibid*. at *12.

58 *Ibid*. at *7.

59 *Ibid*. at *20 – 21.

60 *Ibid*.

61 *Ibid*. at *22.

62 Kate Coleman, "What Is a Deepfake? Reputation: Loss of Credibility and Authenticity", *Status Labs Blog* <https://statuslabs.com/blog/what-is-a-deepfake> ("[T]he impact on reputation does not only affect public figures. While celebrities and politicians may be more likely to be targeted by deepfakes in the first place, they also have more recognition, resources, and status to help control the narrative. However, an ordinary person may struggle to prove the same about themselves if videos, images, or recordings showing them doing something distasteful, inappropriate, or worse comes to light.").

63 Damle, Dukanovic, Lovejoy & Stilliman, "ELVIS Act", *supra* note 28.

64 *Supra* note 10.

that addresses identity-linked harms at scale.[65] A federal statute could standardise core elements, including the definition of "likeness," consent requirements, and safe harbors, while preserving state-law remedies for unique harms. That federal baseline could also facilitate harmonization with emerging global frameworks that recognize identity as a data right or a personality interest, such as in Denmark's proposed likeness-as-copyright reform discussed in Part IV.

A preemptive federal right of publicity seems logical, especially given the increasing intersection of generative AI and other digital technologies with this area of law, which impacts a broad swath of the population.[66] At the same time, critics worry that a sweeping federal law could stifle technological innovation and create legal uncertainty. For instance, restricting anyone from using tools that generate work in the "style" of a person could be overly broad and ambiguous, exceeding the more traditional and limited concern of preventing unauthorised commercial endorsements using someone's name or image.[67] Relatedly, a loosely defined rule could make it difficult to identify whose rights are at stake and to negotiate permissions, potentially discouraging new artists from experimenting creatively for fear of legal repercussions.[68]

Another worry is that codifying and standardising the right of publicity could make it easier to separate the right from the individual it is meant to protect, potentially harming those it was designed to help.[69] This issue was a prominent concern during the recent SAG-AFTRA strike, where many performers expressed fears that powerful entities, such as film studios or music labels, might pressure young or less-experienced artists into signing away their publicity rights.[70] These rights could be buried in standard contracts or waived altogether, exploiting the weaker bargaining position of early-career performers and leaving the right of publicity to serve primarily as a trap for smaller or less-informed creators. Moreover, a federal right may ultimately favour frequent defendants, if the law includes broad exemptions from liability, it could offer them significant protection at the expense of potential plaintiffs.[71]

C. *Copyright Law*

Copyright law, anchored in human authorship and originality, now confronts three fault lines in the age of generative AI. First, copyright law is grounded in the premise

---

[65] § 14:57. Marie A. Kessel "*Holograms are Taking Over the World! An Analysis on Legal Implications Holograms Pose in Right of Publicity and Copyright Law*" in Alexander Lindey, *Lindey on Entertainment, Publishing and the Arts (3rd ed.)* (Thomson Reuters, 2024) (July 2025 Update).

[66] Jennifer E Rothman, "Federal Right of Publicity Takes Center Stage in Senate Hearing on AI", Rothman's Roadmap to the Right of Publicity (July 27, 2023), [Rothman] <https://rightofpublicityroadmap.com/news_commentary/federal-right-of-publicity-takes-center-stage-in-senate-hearing-on-ai/>.

[67] Corynne McSherry, "A Broad Federal Publicity Right Is a Risky Answer to Generative AI Problems", Electronic Frontier Foundation (July 18, 2023) [McSherry] <https://www.eff.org/deeplinks/2023/07/broad-federal-publicity-right-risky-answer-generative-ai-problems>.

[68] *Ibid*.

[69] Rothman, *supra* note 66.

[70] McSherry, *supra* note 67.

[71] Rothman, *supra* note 66.

that works must be the product of human authorship to receive protection.[72] This assumption, codified in both the statutory definition of "author" and the judicial interpretation of originality, becomes an obstacle when dealing with generative AI. The U.S. Copyright Office has repeatedly affirmed that purely AI-generated works are not entitled to protection because they lack the requisite human creative input, despite humans selecting prompts and arranging output.[73]

This position leaves AI-generated content in a peculiar legal limbo. Because it lacks copyright protection, it enters the public domain upon creation.[74] Yet, unlike traditional public domain works whose origins are known and stable, AI outputs may be indistinguishable from human expression or closely resemble protected works. The result is an odd duality: AI-generated works cannot be protected by their creators but may still infringe the rights of others, frustrating creators and rights holders, as neither group has a clear legal path to enforce or defend their interests.

Moreover, the authorship requirement restricts the possibility of asserting rights over emergent, collaborative human-machine works.[75] When a human provides prompts, curates outputs, and contributes iterative adjustments, the boundaries of authorship become blurred. Courts and policymakers are only beginning to explore whether such contributions can meet the "modicum of creativity" standard, or whether they remain too attenuated to qualify.[76]

The second fault line concerns infringement and fair use. The Supreme Court has long held that "ideas," "methods," and "systems" fall outside the scope of protection.[77] Thus, a machine-generated painting that replicates the aesthetics of Basquiat or Hokusai, or a voice model that captures the phrasing and delivery of Morgan Freeman, would likely escape liability under copyright law alone.

---

[72] 17 U.S.C.A. § 102(a) (Copyright protection applies to "original works of authorship" fixed in a tangible medium of expression.). 17 U.S.C.A. § 201(a) states that copyright initially vests in the "author or authors of the work", reinforcing the notion that authorship is tied to human creators. See also *Thaler v. Perlmutter*, 130 F.4th 1039 (2025) (Holding that the statutory framework does not contemplate non-human entities as authors, even in cases involving works created with the assistance of artificial intelligence or other non-human processes.).

[73] U.S. Copyright Office, *Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence* § 503.03(a) (Jan. 30, 2025) ("to qualify as a work of 'authorship' a work must be created by a human being … the Office will not register works produced by a machine … without any creative input or intervention from a human author").

[74] Daryl Lim, "AI & IP: Innovation & Creativity in an Age of Accelerated Change", 52 Akron Law Review 813, at 841 (2018) ("Excluding AI-generated work for protection leaves an economic lacuna, which U.S. IP policy is loath to do.").

[75] *Ibid* at 874 ("In the creative arts, AI learns what we consider to be beautiful and creates permutations both within and outside of those boundaries. At times, it may augment artistic endeavor by providing flashes of inspiration in a collaborative dance. AI evolved from augmentation, to co-creation, to becoming the artist.").

[76] Micaela Mantegna, "ARTificial: Why Copyright Is Not the Right Policy Tool to Deal with Generative AI", (2024), 133 Yale LJ Forum 1126 (noting that "originality has been defined as having 'a modicum of creativity,' which leads us back to debates about what constitutes creativity, and whether a machine can produce an output that could be considered creative"). Note, "Recovering Personality in Copyright's Originality Inquiry" (2025) 138 Harv L Rev 1123 ("Much of the doubt about the future of generative AI and copyright comes from uncertainty about whether copyright's fundamental principles, like originality and creativity, can (or should) accommodate the technology.").

[77] *Eg, Baker v. Selden*, 101 U.S. 99 (1880) (systems for methods of bookkeeping were beyond the scope of copyright protection).

Stylistic mimicry, what was once deemed too abstract for copyright, now holds commercial value.[78] Even when the AI-generated output is not a literal copy, it may mimic the style, tone, or persona of a known artist or performer. This was illustrated by the recent Studio Ghibli phenomenon known as "Ghiblification."[79] In early 2025, users of AI image tools began transforming personal photos and popular memes into the distinctive style of Studio Ghibli, the animation studio founded by Hayao Miyazaki, prompting ethical and legal debates.[80] For instance, what people are thinking of when they say "style" may not be an abstract aesthetic sensibility, but a collection of specific, discernible, and repeatable elements: muted color palettes, round facial features, watercolor-like textures, or visual tropes like floating objects and overgrown landscapes. These stylistic markers function like semiotic signatures, identifiable patterns that audiences immediately associate with a particular creator.

Yet copyright law excludes "style" from protection, categorising it as part of the unprotectable idea or method behind a work rather than its protectable expression.[81] This doctrinal limit creates a mismatch: while the market increasingly values and monetises style as a form of brand identity or cultural currency, the law denies creators a remedy when that style is copied in new, non-literal forms by generative AI. As Bonfiglio noted:

> While we may wish to confidently claim that copyright never protects mere style, the line between unprotectable style and protectable expression can be incredibly thin bordering on nonexistent, especially when dealing with highly distinctive works or specific combinations of elements. Add in high profile and high dollar value uses of an artist's style, and you have a recipe for litigation or threats of litigation, even if ultimately meritless.[82]

This doctrinal limit matters greatly in the age of generative AI, because stylistic mimicry is not merely derivative. It is often the main commercial value.[83] When consumers seek AI tools that "write like Hemingway" or "sing like Drake," they are not purchasing expressive content per se, but rather an approximation of their brand.

---

78 Benjamin LW Sobel, "Elements of Style: Copyright, Similarity, and Generative AI" (2024) 38 Harv JL & Tech 49 (arguing that courts already evaluate stylistic elements under the substantial similarity doctrine and should more explicitly recognize style as protectable expression in light of challenges posed by generative AI.).

79 Justin Bonfiglio, "Ghibli, Ghiblification, Copyright and Style", Authors Alliance Blog (May 8, 2025) ("Courts, comparing specific works, sometimes issue rulings where the copyrightability of style (not standing in isolation, but as a substantial weight considered in the expression of the work) is heavily implicated in infringement findings. This often happens when style is deeply intertwined with other, more clearly protectable elements like specific characters or the overall "total concept and feel" of the works.") [Bonfiglio] <https://www.authorsalliance.org/2025/05/08/ghibli-ghiblification-copyright-and-style/>.

80 *Ibid*.

81 *Eg, McDonald v. West*, 138 F.Supp.3d 448, at 455 (2015).

82 Bonfiglio, *supra* note 79.

83 Riddhi Setty, "AI Imitating Artist 'Style' Drives Call to Rethink Copyright Law", *Bloomberg Law* (May 31, 2023) (quoting Robert Brauneis that "this personal style of individual creators could be imitated as well and as inexpensively as we now have with AI"), <https://news.bloomberglaw.com/ip-law/ai-imitating-artist-style-drives-call-to-rethink-copyright-law>.

Copyright's focus on originality and fixation fails to account for this dynamic. This underscores how AI can disseminate a recognisable "artistic language" at scale and raises new challenges for copyright law, which traditionally targets literal copying rather than style appropriation.

The right of publicity can partially fill this gap, especially where the output invokes a recognisable identity.[84] However, for anonymous or non-celebrity creators, there may be no remedy. Their style, which is refined over the years, encoded into publicly available work, may become fair game for model ingestion and imitation without credit or compensation.

With respect to fair use, AI developers argue that ingestion of works for statistical patterning constitutes fair use, analogising the process to Google Books' digitization in *Authors Guild v. Google, Inc.,*[85] or the creation of searchable databases like those in *Kelly v. Arriba Soft* and *Perfect 10 v. Amazon*.[86] Indeed, it is a feature that *Bartz* heralded as "among the most transformative many of us will see in our lifetimes."[87]

The difficulty, however, is that unlike search engines or thumbnail repositories, generative AI systems do not merely index or point users toward protected content. They internalise the stylistic and structural attributes of the training data, enabling them to generate outputs that may be stylistically identical or even compositionally similar to their inputs.

Moreover, jurisdictional mismatches between the US's sectoral, doctrine-specific approach and the European Union's more centralised, rights-based frameworks, such as the GDPR and the AI Act, raise questions about cross-border enforceability, consistency, and legal certainty. As Scannell and Moore noted,

> Yet the [*Bartz*] ruling also throws an emerging tension with European law into sharper relief. Under the EU's Copyright in the Digital Single Market Directive, rightsholders can reserve rights against text and data mining for commercial purposes. If a US-based company circumvents such reservations by scraping European works or sidestepping opt-outs under Article 4, American courts could potentially treat that conduct as functionally equivalent to piracy. The judgment leaves the possibility that acquiring material in breach of non-U.S. rights reservations, even if the end use is technically transformative, could taint the

---

[84] *Andersen v. Stability AI Ltd.*, 700 F.Supp.3d 853 (2023) (Plaintiffs argued AI systems appropriated their names and artistic styles to market AI-generated art, thereby violating their publicity rights, but the court held that they did not sufficiently allege right-of-publicity claims under California common law or statute.). See also *Facenda v. N.F.L. Films, Inc.*, 542 F.3d 1007 (2008) (Right of publicity is not preempted by copyright law when the claim focuses on the misuse of a person's identity rather than the control of a copyrighted work.).

[85] *Authors Guild v. Google, Inc.*, 804 F.3d 202 (2d Cir., 2015).

[86] *Kelly v. Arriba Soft Corp*., 336 F.3d 811, at 819 (9th Cir., 2003); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, at 1165 (9th Cir., 2007).

[87] *Bartz v. Anthropic PBC*, 787 F. Supp. 3d 1007, 1032 (N.D. Cal. 2025). See also *ibid.*, at *17 ("Authors' complaint is no different than it would be if they complained that training schoolchildren to write well would result in an explosion of competing works. This is not the kind of competitive or creative displacement that concerns the Copyright Act. The Act seeks to advance original works of authorship, not to protect authors against competition.").

> entire process under US law because the decisive test turns on how the input was sourced, not just how it is processed.[88]

Relatedly, two recent US district court decisions diverge on the fourth fair use factor—market impact. While Judge Alsup in *Bartz* downplayed competitive harm by analogising AI training to human learning,[89] Judge Chhabria in *Kadrey v. Meta* emphasised the risk of "market dilution," warning that LLMs could flood the creative market with low-cost substitutes.[90] Notably in the face of concerns over dampening innovation, Judge Chhabria remarked that

> So if it isn't fair use for Meta and other LLM developers to use copyrighted books as training data without permission, they won't have to stop working on their LLMs altogether. They'll just have to pay for licenses or use books that aren't copyrighted. Either way, it may be that LLM companies move somewhat more slowly or make somewhat less money. But the suggestion that the growth of LLM technology would come to a halt (or anything close) doesn't pass the straight face test.[91]

However, he granted summary judgment for Meta due to plaintiffs' failure to provide empirical evidence of market harm, illustrating the evidentiary hurdles in framing AI training as a threat to original expression.[92]

Further complicating matters, the composition of AI training sets remain opaque.[93] This lack of transparency prevents rights holders from assessing whether their works were used, and if so, whether they were altered in meaningful ways. Even under the prevailing liberal fair use regime post-*Kadrey* and *Bartz*, the concealment of source data undermines trust and precludes the balancing necessary for adjudicating claims.

A creator alleging that an AI-generated output mimics their work may be unable to determine whether their content was used in training unless the developer voluntarily discloses dataset composition or model weights. Even where disclosure

---

88 Barry Scannell & Leo Moore, "Artificial Intelligence and Copyright: Significant U.S. Judgment", *Lexology* (July 1, 2025), <https://www.lexology.com/library/detail.aspx?g=dba6083e-2ced-4ddc-97e8-44b9d74be2cc>.

89 Bartz, 787 F. Supp. 3d, at 1032 (N.D. Cal. 2025) ("Authors next contend that training LLMs displaced (or will) an emerging market for licensing their works for the narrow purpose of training LLMs. Anthropic argues that transactional costs would exceed Anthropic's expected benefit from any such bargain, prompting it to cease dealing with any rightsholders or else to cease developing such technology altogether. Our record could support either account—so this order must assume Authors are correct. A market could develop. Even so, such a market for that use is not one the Copyright Act entitles Authors to exploit.").

90 *Kadrey v. Meta Platforms, Inc*., 788 F. Supp. 3d 1026, 1055 (N.D. Cal. 2025). ("This case, unlike any of those cases, involves a technology that can generate literally millions of secondary works, with a miniscule fraction of the time and creativity used to create the original works it was trained on. No other use—whether it's the creation of a single secondary work or the creation of other digital tools—has anything near the potential to flood the market with competing works the way that LLM training does. And so the concept of market dilution becomes highly relevant.").

91 *Ibid*. at 1059.

92 *Ibid*.

93 Daryl Lim, "AI, Equity, and the IP Gap", (2022) 75 SMU L Rev 815, at 838 (Discussing the implications of algorithmic opacity.).

occurs, technical complexity often obscures the causal chain between ingestion and output. Courts, lacking clear benchmarks or expert consensus on what constitutes impermissible similarity in style or structure, struggle to apply traditional infringement frameworks to probabilistic generation.

Labelling requirements, dataset registries, or opt-out databases may provide partial relief but do not fully address the systemic opacity of generative models.[94] Without meaningful access to underlying data and model behavior, both plaintiffs and courts are left to speculate on the degree of similarity between inputs and outputs. This evidentiary gap poses serious challenges to enforcing intellectual property rights and evaluating fair use claims. The result is a regime in which the burden of proof disproportionately rests on creators, while platforms benefit from plausible deniability. This structural imbalance underscores the need for stronger transparency obligations, robust auditing mechanisms, and potentially, fiduciary duties of care for data stewardship in high-risk AI applications.

The third fault line is that transaction costs will rise in the absence of a licensing pathway. Deezer, a major global streaming platform, reported that 18 percent of daily uploads are now AI-generated, totalling over 20,000 AI-created tracks per day in 2025, marking nearly a twofold increase from earlier figures.[95] Copyright lawsuits filed against AI developers in the US now exceed two dozen.[96] These suits, which span issues from unauthorised training data use to the reproduction of stylistic or sonic signatures, reflect not only heightened enforcement efforts but also the breakdown of informal market norms that once facilitated low-friction licensing. Without scalable and interoperable licensing solutions, creators, rights holders, and platforms alike face mounting legal exposure and costly negotiations over rights that were once implicit or routinised.

Given these limitations, a single doctrinal response, including expanding copyrightability, narrowing fair use, or revising the originality requirement, will likely be insufficient. As discussed above, the No AI FRAUD Act proposes a new federal right allowing individuals to sue AI companies for unauthorized use of their creative output or likeness.[97] While this bill represents a significant step toward recognising identity-based harms in generative AI, its narrow focus and uncertain scope underscore the need for more systemic, cross-cutting solutions. Likewise, the NO FAKES Act, while advancing important protections against unauthorised digital replicas, is limited in scope. It primarily targets celebrity likeness and audiovisual performances, leaving unaddressed broader concerns around style mimicry, dataset provenance, and the structural opacity of generative AI systems.

A layered, pluralist framework is more promising. Copyright law should maintain its core commitments to creativity and public domain access. However, it should also be supplemented by targeted interventions, including disclosure mandates, data

---

[94] Databases used to train AI models are kept confidential, making transparency efforts insufficient to pierce the opacity of the actual training data and provenance. See *ibid*.

[95] "Deezer Reveals 18% of All New Music Uploaded to Streaming Is Fully AI-Generated", *Deezer Newsroom* (Apr. 16, 2025), <https://newsroom-deezer.com/2025/04/deezer-reveals-18-of-all-new-music-uploaded-to-streaming-is-fully-ai-generated/>.

[96] Ben Lutkevich & Rosa Heaton, "AI Lawsuits Explained: Who's Getting Sued?", *TechTarget* (July 7, 2025), <https://www.techtarget.com/whatis/feature/AI-lawsuits-explained-Whos-getting-sued>.

[97] *Supra* note 10.

stewardship obligations, and collective licensing schemes that enable rights holders to participate in AI ecosystems without having to litigate every instance of unauthorized use. Here, one possibility is to develop a hybrid licensing system akin to compulsory licensing in the music industry.

As one *Financial Times* commentary put it, moving "from ad hoc deals to a broader market for training licenses" through "supporting licensing markets" would offer a "win-win solution" that balances sustained access for AI developers with fair compensation and control for creators.[98] Rights holders could register their content for AI training, receive standardised fees, and opt out if desired. Another is to redefine certain forms of AI-enabled replication, such as voice and likeness synthesis, as implicating multiple rights simultaneously, triggering parallel remedies in publicity, copyright, and data law.

In short, copyright's doctrinal architecture was built for static works, human authors, and identifiable copying. It must evolve to meet the demands of AI. But can it or, more importantly, should it? Rather than stretching it beyond recognition, we can preserve its integrity by allowing neighbouring doctrines to carry the weight in adjacent domains. A data right, as proposed in the next section, offers one such complementary mechanism. While copyright focuses on original expression fixed by human authors, a data right targets the upstream flows of identity-linked or personally attributable information that feed generative AI systems. It enables individuals to assert control over how their data, including likeness, voice, style, or digital traces, is used in model training, even when that use falls outside copyright's scope.

Unlike copyright, which often requires costly enforcement and proof of substantial similarity for infringement liability,[99] a data right could operate through transparency obligations, opt-in or opt-out mechanisms, and graduated remedies based on the scale and context of use. In doing so, it would provide a flexible, harm-based layer of accountability that complements existing doctrines without forcing copyright law to bear the full weight of regulating synthetic media. This layered approach allows copyright to retain its coherence while enabling a broader regulatory ecosystem attuned to the realities of AI-generated content.

IV. A Data Right for the Age of Generative AI

Part IV proposes a federal "data right" as a harmonising framework to supplement existing privacy, publicity, and copyright regimes. Rather than displacing these doctrines, the data right aims to integrate their most effective features while addressing their shared limitations in the context of generative AI. This data right can also be considered by other jurisdictions facing similar issues. This Part outlines how the data right would function as a safeguard to empower individuals, increase transparency, and guide institutional behavior. It details the right's definitional

---

[98] "AI copyright wars need a market solution", *Financial Times* (Mar. 4, 2025), <https://www.ft.com/content/304d660f-6cac-4e38-a6d5-d8d98f5770fb>.

[99] For a discussion of the substantial similarity doctrine, see Daryl Lim, "Substantial Similarity's Silent Death", (2021), 48 Pepperdine Law Review 713 and its sequel, Daryl Lim, "Saving Substantial Similarity", (2021), 73 Fla L Rev 591.

scope, operational mechanics, and potential remedies, and then situates it within the broader legal landscape. The discussion also anticipates practical challenges, including enforcement design, doctrinal overlap, and concerns about federal preemption, offering strategies such as safe harbors, priority rules, and evidentiary burdens to mitigate these risks.

A. *Situating the Data Right*

To ensure the proposed data right functions as a coherent supplement rather than a source of conflict, its relationship with existing federal regimes warrants careful delineation. First, the right should be crafted to avoid preemption under the Copyright Act by expressly excluding claims based on original expression or fixed works, focusing instead on identity-linked attributes not protected under copyright law, such as voice timbre or biometric traits.[100] Likewise, to survive Dormant Commerce Clause scrutiny, the statute should establish a clear federal baseline while preserving limited state-level augmentation only where it does not burden interstate commerce.[101]

Second, the regime must anticipate evidentiary challenges. In black-box generative systems, individuals often cannot prove that their data was ingested or how it contributed to a specific output.[102] To address this asymmetry, the statute should authorise presumptions or burden-shifting frameworks when high-fidelity likeness is demonstrated, compelling developers to prove either non-use or authorised use.

Third, while doctrinal redundancy can promote resilience through overlapping protections, it also carries risks of inefficiency, legal uncertainty, and overdeterrence. Without coordination mechanisms, individuals and developers alike may face duplicative liability, conflicting standards, or inconsistent remedies across federal, state, and private enforcement channels. To some extent, this complexity is not without precedent. US intellectual property law routinely accommodates overlapping rights. Consider how design patents, trade dress, and copyright can all apply to a single product. Rather than being a flaw, this redundancy enhances robustness. At the same time, the data right should be implemented alongside mechanisms that clarify the relationship between overlapping regimes.[103]

By specifying the scope, triggers, and enforcement mechanisms of the data right, the proposal aims to coordinate doctrinal coverage, ensuring that each right

---

[100] Midler, *supra* note 44 at 462 (while a recording may be protected, the voice itself is not copyrightable expression.); Laura K. Donohue, "Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age" (2012) 97 Minn L Rev 407 at 544 (biometric data such as voiceprints or facial data are recognized as non-copyrightable identity-linked characteristics, distinct from expressive works).

[101] Elizabeth Earle Beske, "Horizontal Federalism & the Big State "Problem"" (2024) 65 Boston College L Rev 2685 at 2708 – 2721.

[102] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, 2015). See also Daryl Lim, "AI, Equity, and the IP Gap", (2022) 75 SMU L Rev 815 at 855 (discussing the importance of equity audits).

[103] *Kohler Co. v. Moen Inc.*, 12 F.3d 632 (7th Cir., 1993) (A product's different qualities can be protected simultaneously or successively by intellectual property rights, as they serve distinct purposes and operate under different legal standards.).

addresses a distinct dimension of identity-linked harm while reducing gaps in protection. For example, safe harbor provisions could shield developers who adopt certified technical safeguards from liability under multiple doctrines.[104] Priority rules could specify when the data right should yield to copyright or publicity claims, depending on the nature of the harm.[105] Preemption thresholds could also be defined to preserve state innovation while avoiding doctrinal conflict. Rather than eliminating overlap, these tools would manage it, thereby preserving pluralism's benefits while reducing its frictions.

Fourth, the proposal for a data right anticipates objections, such as concerns that it may stifle innovation or render identity into corporate property. These concerns are addressed through careful scope limitations, transparency safeguards, and a review mechanism that allows for the law to be adapted over time. To address concerns about overreach, the data right would be narrowly scoped to cover only personal data such as realistic voice, image, or biometric replication rather than incidental or transformative uses.

Fifth, transparency safeguards, including clear disclosure obligations and audit trails, ensure that individuals understand when and how their identity-linked data is being used, preventing covert exploitation.[106] To avoid the ossification of rights or the entrenchment of private control over identity traits, the proposal includes a built-in review mechanism, modelled after sunset clauses or periodic impact assessments, that mandates reassessment of the law's effectiveness, unintended consequences, and technological relevance.[107] Together, these design features ensure that the data right remains protective without becoming punitive, adaptive without being unstable, and equitable without chilling legitimate innovation.

The proposed data right could support cooperative mechanisms that reduce the cost and complexity of asserting rights at scale. One promising avenue is the development of collective rights organisations, like copyright collectives or performing rights organisations that could license identity-linked data on behalf of creators, negotiate terms with AI developers, and pursue enforcement actions when necessary.[108] For digital performers, voice actors, and creators with limited bargaining power, such institutions could serve as intermediaries in licensing negotiations, model audits, or litigation, lowering transaction costs and ensuring that the benefits of the data right are accessible beyond high-profile cases.[109]

---

[104] Jeremy Bloomstone, "From Principles to Principals—Establishing Safe Harbors & Regulating the Ethical Development of Artificial Intelligence Systems", *Center for Legal & Court Technology* (Nov. 21, 2024), <https://www.legaltechcenter.net/2024/11/21/from-principles-to-principals-establishing-safe-harbors-regulating-the-ethical-development-of-artificial-intelligence-systems/>.

[105] *Eg, Jackson v Roberts*, 972 F.3d 25 (2d Cir., 2020) (adopting the copyright preemption doctrine to bar the plaintiff's state right of publicity claim.).

[106] *Eg, American Federation of Government Employees, AFL-CIO v. U.S. Office of Personnel Management*, 777 F.Supp.3d 253 (S.D.N.Y., 2025) (granting improper access to legally protected data constitutes a harm resembling intrusion upon seclusion, even without further use or review of the data.).

[107] *Eg, AG der Dillinger Huttenwerke v. U.S.,* 26 C.I.T. 298 (2002).

[108] Copyright Clearance Center, *CCC Launches Collective AI License*, Velocity of Content blog (July 19, 2024), <https://www.copyright.com/blog/ccc-launches-collective-ai-license/>.

[109] *Eg, American Soc. of Composers, Authors and Publishers v. Showtime/The Movie Channel, Inc.*, 912 F.2d 563 (2d Cir., 1990).

B. *Key Components*

The data right should include five key features: (1) Informational self-determination, (2) Disclosure obligations, (3) Access and deletion rights, (4) Redress mechanism, and (5) Limited excludability.

1. *Informational Self-determination*

At the core of the data right is the principle that individuals should retain meaningful agency over how their identity-linked data, such as voice, likeness, biometric markers, or expressive style, is used in AI systems. This entails an explicit, opt-in consent requirement before such data may be used for training or generation purposes. Unlike passive notice or implied consent models, which often rely on lengthy privacy policies or default platform settings, opt-in consent demands affirmative, informed permission.[110] It ensures that individuals are not unknowingly subjected to identity extraction and replication. This risk is especially acute when AI systems generate outputs that are hyper-realistic, emotionally evocative, or commercially exploitable.

This approach draws on longstanding privacy principles of informational self-determination and informed autonomy. It aligns with best practices in data protection frameworks such as Article 6(1)(a) of the GDPR, which requires consent to be freely given, specific, informed, and unambiguous.[111] Applying this standard to identity-linked AI promotes trust, transparency, and fairness, particularly in domains such as entertainment, politics, or personalised services. Importantly, the obligation would apply only to identity-sensitive uses, such as those involving synthetic impersonation or realistic simulations, rather than to all data generally. This calibration maintains operational feasibility for developers while offering robust protections where the risk of harm is highest.

The proposed data right draws normative strength from multiple strands of US constitutional tradition. The principle of decisional autonomy has long been recognised in substantive due process jurisprudence as a liberty interest protecting intimate personal choices.[112] Just as the Constitution shields individuals from unwanted

---

[110] *Eg, Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir., 2024) (requiring the defendant to demonstrate that the circumstances, considered as a whole, show knowing authorisation by the plaintiff.); *National Cable & Telecommunications Ass'n v. F.C.C.,* 555 F.3d 996 (DC Cir., 2009) (noting that opt-in consent presumes consumers do not want their information shared unless they expressly indicate otherwise, contrasting it with opt-out schemes that presume the opposite.); *Sosa v. Onfido, Inc.,* 600 F.Supp.3d 859 at 884 (2022) (distinguishing between consent to one type of data collection (*eg,* photographs) and consent to another (*e.g*., biometric data), underscoring the need for specific, informed consent for each practice.).

[111] GDPR, *supra* note 27 at art. 4(11), 6(1)(a), 7, and Recital 32 (Consent must be "freely given, specific, informed and unambiguous" and signalled by a "clear affirmative action," such as an unchecked checkbox or clicking "I agree").

[112] *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 at 225- 228 (2022) (Decisional autonomy has been recognised as a liberty interest under substantive due process, particularly in the context of family, marriage, and reproductive decisions, but historical and traditional considerations, and recent developments limit its scope.).

government intrusion into decisions about health, family, and identity,[113] the data right aims to protect individuals from nonconsensual appropriation of their digital selves by private actors. It also reflects dignitary interests embedded in privacy tort doctrine and First Amendment jurisprudence, which guard against reputational injury, false attribution, and compelled association.[114] Additionally, the right promotes expressive agency by enabling individuals to participate in decisions about how their identity-linked data is used, particularly where AI systems generate outputs that may appear to speak on their behalf or in their likeness.[115] While grounded in these personal liberty and speech values, the right also addresses structural concerns, particularly the asymmetry of power between individuals and developers.[116] It thus aims to preserve human identity as a source of expressive and moral worth, not merely as an input in algorithmic optimisation.

Moreover, opt-in consent reinforces the expressive and dignitary interests protected by the right of publicity and privacy laws, while providing a forward-looking mechanism to address novel harms that fall outside existing doctrines. In effect, it reasserts individual control over the attributes that make one recognisable and unique in a digital environment where such attributes are increasingly commodified. Without such consent, identity risks becoming a mere input that is disaggregated, decontextualised, and redeployed at scale without the individual's knowledge, let alone participation.

This consent-based model finds support in US law. BIPA requires written informed consent before collecting biometric identifiers such as facial geometry or voiceprints, and has served as a national template for regulating identity-linked data.[117] Similarly, the ELVIS Act mandates affirmative consent before an individual's voice or likeness may be replicated by AI, and offers statutory damages and postmortem rights.[118] These statutes demonstrate the feasibility and normative appeal of opt-in models tailored to identity-based harms and offer valuable lessons for structuring a federal data right responsive to the realities of generative AI.

---

[113] *Eg*, *Whalen v. Roe*, 429 U.S. 589 at 599–600 (1977) (recognising an individual's interest in avoiding disclosure of personal matters).

[114] *Eg*, *Cohen v. California*, 403 U.S. 15 at 24–26 (1971) (discussing compelled expression and personal dignity); *Time, Inc. v. Hill*, 385 U.S. 374 at 383–84 (1967) (recognising reputational harms as a legitimate privacy interest).

[115] *Eg*, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 at 341–342 (1995) (affirming the right to control how one speaks and is identified in public discourse); *Roberts v. United States Jaycees*, 468 U.S. 609 at 618–19 (1984) (recognising individual interests in expressive identity within association).

[116] Tao Huang, "Free Speech Capability", (2024), 37 Harv Hum Rts J 1 at 1; Jack M. Balkin, "Free Speech Versus the First Amendment", (2023), 70 UCLA L Rev 1206 at 1206.

[117] BIPA, *supra* note 26, at 14/15(b).

[118] ELVIS Act, *supra* note 28 at § 47-25-1105(a) (precluding AI-generated voice or likeness replication without consent); § 47-25-1105(a)(2) & (3) (new secondary liability); § 47-25-1106(a)–(d) (providing civil remedies); § 47-25-1105(b) (Establishes criminal liability for violations as a Class A misdemeanor, punishable by up to 11 months and 29 days imprisonment and a fine up to $2,500).

2. *Disclosure Obligations*

Developers would be required to disclose, through public-facing documentation or registries, whether identity-linked data was included in training sets. Disclosure enhances both user trust and legal enforceability: individuals cannot meaningfully assert their rights unless they know whether and how their identity has been implicated. It also provides a baseline for regulators and courts to assess the extent of potential misuse. This disclosure obligation aligns with calls for accountability in the design of AI systems.[119]

Beyond transparency, disclosure acts as a gatekeeping mechanism. By obligating developers to record and publish the sources and types of data used in training, it creates a paper trail that enables oversight and deters opportunistic exploitation. Analogous obligations already exist in other regulatory contexts. Under Articles 13 and 14 of the GDPR, data subjects have a right to be informed about the collection and use of their personal data, including information about the data's origin, its recipients, and the purposes of processing.[120] Similarly, the EU AI Act requires developers of high-risk AI systems to maintain technical documentation detailing their training datasets, intended uses, and risk mitigation strategies.[121]

In the US, sectoral privacy statutes, such as BIPA, already require businesses to disclose the categories of personal information they collect and how they use it.[122] The Federal Trade Commission (FTC) has also emphasised transparency and explainability as key principles of trustworthy AI design. In recent guidance, it warned developers to avoid making unsubstantiated claims about training datasets and to ensure they know "what data [their] model was trained on" to avoid deceptive or unfair practices under Section 5 of the FTC Act.[123] In the intellectual property

---

[119] Shayne Longpre et al., "Data Authenticity, Consent, and Provenance for AI Are All Broken: What Will It Take to Fix Them?" (2024) *arXiv Cornell University* Release 2 (arguing that AI training data remains opaque and calling for standardised data provenance frameworks to enable developer disclosure and public accountability).

[120] GDPR, *supra* note 27.

[121] Regulation (EU) 2024/1381 of the European Parliament and of the Council of 13 March 2024 on Artificial Intelligence, 2024, (Europe), at Article 10 (mandating high-risk AI systems must be developed using high-quality datasets that are representative, error-free, and accompanied by documentation of collection processes, origin, preparation steps (eg, labelling, annotation), and statistical assumptions) and Article 11 (requiring that comprehensive technical documentation be drawn up *before* the system is placed on the market or put into service and maintained throughout its life cycle, including information on data provenance, system architecture, developer assumptions, human oversight mechanisms, and risk assessment procedures.).

[122] 740 ILCS (United States, Illinois) 14/15(b) (Private entities to provide written notice regarding the biometric information being collected and its intended purpose and retention period, and must obtain written consent before collection); 740 ILCS (United States, Illinois)14/15(a) (Private entities to create and publicly post a retention and destruction schedule before collecting biometric data.).

[123] "Transparency and AI: FTC Launches Enforcement Actions Against Businesses Promoting Deceptive AI Product Claims", *Lathrop GPM LLP*, (Apr.16, 2025), <https://www.lathropgpm.com/insights/transparency-and-ai-ftc-launches-enforcement-actions-against-businesses-promoting-deceptive-ai-product-claims/> (noting the FTC's enforcement sweep, "Operation AI Comply," targeting misleading and unsubstantiated claims about AI product performance under Section 5(a) of the FTC Act).

domain, metadata standards for attribution, licensing, and provenance play a vital role in collective rights management and copyright enforcement.[124]

A US data right might be based on similar principles as laws in other countries. However, differences in how broadly it applies, how it is enforced, and how identity-related data is classified, could nonetheless create challenges for transferring data across borders, coordinating enforcement, and recognising each other's rights internationally. For example, while the GDPR treats data protection as a fundamental right administered by data protection authorities, a US data right would be rooted in statutory torts and administered by the FTC or private actors.[125] To mitigate these risks, the US framework would need to incorporate transnational design principles, such as data portability, standardised documentation, and cross-border redress protocols, that enable the data right to function as a modular component within broader global governance ecosystems.

Uniform disclosure requirements could enhance comparability, reduce compliance costs, and facilitate coordinated oversight across federal and state authorities. Disclosure obligations could be operationalised through standardised documentation tools already gaining traction in the AI research and development community. For instance, "Datasheets for Datasets," proposed by Timnit Gebru et al., call for structured documentation that provides context about how and why a dataset was created, its composition, and its intended uses.[126] Similarly, "Model Cards for Model Reporting," developed by Mitchell et al., offers templates for communicating the intended use cases, limitations, and training details of AI models.[127] These tools could be adapted or mandated by regulators for identity-linked applications. Thus, while structured heterogeneity fosters doctrinal innovation and resilience, there are domains involving technical standards and systemic risk where convergence can enhance fairness, efficiency, and regulatory coherence.

3. *Access and Deletion Rights*

Modelled after existing privacy regimes such as the GDPR and California's CCPA, the data right would empower individuals to request access to their identity-linked data used in training datasets, and to demand its removal under defined circumstances. By offering individuals the ability to correct or delete identity-based

---

[124] *Eg, Stevens v. Corelogic, Inc.*, 194 F.Supp.3d 1046 (2016) (metadata embedded in image files was noted as crucial for identifying copyright information and tracking ownership, even though the absence of metadata did not directly lead to copyright infringement); *Murphy v. Millennium Radio Group LLC*, 650 F.3d 295 (2011) (copyright management information embedded in digital works is not limited to automated copyright protection systems but serves broader rights management functions.).

[125] GDPR, *supra* note 27 at Recital 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right."); *infra* Part IVB.

[126] Timnit Gebru et al., "Datasheets for Datasets", *arXiv preprint 1803.09010*, (Dec. 1, 2021), <https://arxiv.org/abs/1803.09010> (proposing standardised datasheets to accompany datasets documenting motivation, composition, provenance, intended use, and limitations).

[127] Margaret Mitchell et al., "Model Cards for Model Reporting", *arXiv:1810.03993 v2* (Jan. 14, 2019), <https://arxiv.org/abs/1810.03993> (proposing transparent documentation accompanying AI models, including intended use, performance metrics disaggregated across demographic groups, and context of use).

records, the right functions as an *ex ante* safeguard against reputational harm and post hoc misuse. It also fosters a feedback mechanism for developers, enabling better dataset curation and risk mitigation.

The logic of these access and deletion rights mirrors the "right to know" and "right to be forgotten" provisions embedded in Articles 15 and 17 of the GDPR.[128] Under these provisions, individuals can obtain confirmation of whether their personal data is being processed, access copies of that data, and request its erasure. The CCPA similarly grants California residents the right to know what personal information businesses collect about them and to request its deletion, subject to specific exceptions.[129]

Translating these principles into the AI context, the data right would give individuals the ability to determine whether their voice, likeness, biometric markers, or expressive traits have been ingested by generative systems whether directly, if scraped from a public video or indirectly, if learned through derivative materials. If so, the individual could request a record of that data's use, its source, the training model it informed, and the purpose for which it was deployed. Where justified, as in cases involving non-consensual collection, reputational injury, or sensitive attributes, the individual could also request removal, triggering a duty for developers to retrain or otherwise mitigate the effects of retention.

Granted, technical implementation may pose challenges, especially for large-scale models that internalise data in non-traceable ways.[130] However, these rights can still be meaningfully enforced through hybrid mechanisms. For example, developers could be required to maintain hashed records of training data sources and use data provenance tracking to link model outputs to identifiable training inputs.[131] Where full deletion is infeasible, synthetic mitigation techniques such as fine-tuning or suppression filters could reduce downstream risk.[132]

From a governance perspective, access and deletion rights also serve a system-level function. They create pressure for responsible data curation, incentivise documentation, and reduce the prevalence of low-quality or illegally obtained datasets.[133] For regulators and courts, they supply a clear procedural pathway for evaluating

---

[128] GDPR, *supra* note 27 at article 15(1)–(3) (granting data subjects the right to obtain from the controller confirmation of whether personal data concerning them is being processed, and, if so, access to the data and details including purposes of processing; categories of personal data; recipients; storage period; right of rectification, erasure, restriction, or objection; and meaningful information about automated decision-making and its significance); article 17(1)–17(2) (data subjects can have personal data erased without undue delay when one of several grounds applies, eg, data no longer necessary, withdrawal of consent, objection to processing, or unlawful processing—and requiring controllers who have made data public to notify other controllers to erase links or copies).

[129] Cal. Civ. Code 2024 (United States, California) §§ 1798.100–1798.199.100 (California Consumer Privacy Act, as amended by the California Privacy Rights Act).

[130] Bamidele Matthew, "Model Versioning and Reproducibility Challenges in Large-Scale ML Projects", (2025), *Advances in Engineering Software*, <https://www.researchgate.net/publication/392595159>.

[131] Sebastian Schelter, Sudeeptha Guha & Stefan Grafberger, "Automated Provenance-Based Screening of ML Data Preparation Pipelines", (Datenbank Spektrum, 2024), vol 24, <https://doi.org/10.1007/s13222-024-00483-4>.

[132] *Eg,* Jie Ren et al., "SoK: Machine Unlearning for Large Language Models", *arXiv* (June 10, 2025), <https://arxiv.org/html/2506.09227v1>.

[133] OECD, "Going Digital Guide to Data Governance Policy Making" (2022), at 9, <https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/going-digital-guide-to-data-governance-policy-making_28519d90/40d53904-en.pdf>.

claims and remedying misuse without resorting to intellectual property or tort doctrines. For individuals, they translate abstract principles of autonomy and dignity into actionable entitlements in the face of AI systems that would otherwise treat their identities as raw material.

4. *Redress Mechanisms*

In cases of distributed harm, such as viral AI-generated impersonations or persistent misuse of voice clones, private enforcement becomes essential, especially where regulatory agencies may lack the resources or mandate to intervene directly. The data right would enable private lawsuits, offering statutory damages and injunctive relief for unauthorised or injurious uses of identity-linked data. These remedies mirror those found in copyright law, where statutory damages address the difficulty of proving economic harm, and injunctive relief halts further misuse.[134]

A private right of action serves multiple functions. First, it empowers individuals to vindicate their rights without relying solely on under-resourced government bodies.[135] Second, it shifts the burden of internalising the costs of misuse to developers and platforms, incentivising more careful data governance and responsible AI design.[136] Third, it enables the legal system to establish precedents in a rapidly evolving technological landscape, providing courts with concrete fact patterns through which to interpret the contours of emerging rights.[137]

The logic behind statutory damages is especially salient in the AI context. When identity-linked harms occur, such as unauthorised voice synthesis or hyper-realistic digital impersonations, quantifying economic loss can be exceedingly difficult. The damage may be reputational, dignitary, or affect future opportunities in ways that are speculative or diffuse. As in copyright law, statutory damages would serve as a proxy for actual harm, deterring misuse even in the absence of precise valuation.[138]

Injunctive relief is equally critical. In an era of rapid content dissemination, a viral AI-generated deepfake can reach millions of viewers before takedown tools

---

[134] 17 U.S.C. (United States) § 504(c) (Allowing plaintiffs to pursue fixed monetary awards ranging from $750 to $30,000 per work, and up to $150,000 if willful even when actual economic harm or infringer profit is hard to establish); 17 U.S.C. (United States) § 502 (empowering courts to prevent ongoing or future infringement, especially where irreparable harm to the copyright owner is likely.).

[135] Lauren Henry Scholz, "Private Rights of Action in Privacy Law" (2022) 63 Wm & Mary L Rev 1639 (arguing that private rights of action are the most direct regulatory access point to the private sphere.).

[136] Konrad Degen & Alexander Gleiss, "Time to Break Up? The Case for Tailor-Made Digital Platform Regulation Based on Platform-Governance Standard Types" (2025) 35 Electronic Markets, <https://link.springer.com/article/10.1007/s12525-024-00747-7>. (emphasising the need for platform governance regulation that shifts the burden of proof for regulatory compliance from regulators to platform owners.).

[137] BJ Ard, "Making Sense of Legal Disruption" Wis L Rev (2022) at 43 ("legal disruption arises when technological change presents problems that are difficult to resolve through standard processes of making, enforcing, and updating the law").

[138] *Energy Intelligence Group, Incorporated v. Kayne Anderson Capital Advisors, L.P.*, 948 F.3d 261, 273 (2020) (statutory damages serve as a remedy for cases where proving actual harm is challenging, stating that they are designed "to give the owner of a copyright some recompense for injury done him, in a case where the rules of law render difficult or impossible proof of damages or discovery of profits.").

or fact-checking interventions are triggered.[139] Courts need the authority to issue immediate relief such as removing the offending content, halting model deployment, or prohibiting further use of identity-linked data before the harm becomes irrevocable. This mirrors the logic in right of publicity cases, where courts have granted injunctions to prevent the ongoing exploitation of a person's likeness.[140]

To further strengthen enforcement, Congress could model the data right's private action mechanism on frameworks like BIPA, which allows any "person aggrieved" by a violation to bring a civil action and seek liquidated damages, attorneys' fees, and injunctive relief.[141] Importantly, the availability of private enforcement must be paired with procedural safeguards to prevent abuse while ensuring access to justice. These may include standing thresholds, anti-Strategic Lawsuit Against Public Participation (SLAPP) protections, or notice-and-cure provisions for inadvertent first-time violations.[142] Taken together, a well-designed private right of action would balance deterrence, redress, and innovation, providing individuals with meaningful remedies while signalling that the misuse of identity in the AI era carries real legal consequences.

More broadly, the need for a data right cannot be divorced from the structural realities of the digital economy. The same firms that develop generative AI models often control the app stores, cloud infrastructure, social media platforms, and content distribution channels through which synthetic outputs are deployed and monetised.[143] This vertical and horizontal concentration enables dominant players to internalise control over both upstream training data and downstream market access, magnifying existing power asymmetries.[144] Individuals seeking to challenge misuse

---

[139] Mika Westerlund, "The Emergence of Deepfake Technology: A Review" (2019) 9 Technology Innovation Management Review 39, <https://doi.org/10.22215/timreview/1282> (discussing how "convincing deepfakes can quickly reach millions of people and have negative impacts on our society").

[140] *Ali v. Playgirl, Inc*., 447 F.Supp. 723 (1978) (injunctive relief is appropriate when there is a likelihood of recurrent violations of a public figure's rights, including the unauthorized use of their likeness.).

[141] BIPA, *supra* note 26 (BIPA enforcement provision); see also *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197 at 1207 (Ill. 2019) (affirming that mere statutory violation of BIPA suffices to confer standing).

[142] See generally Richard J Pierce, Jr., "Making Sense of Procedural Injury" (2009) 62 Admin L Rev. 1; Harry W R Chamberlain & Lisa M Chait, "The "Nuts and Bolts" of Anti-SLAPP: What Every Lawyer Should Know About Anti-SLAPP Motions" (2017), Buchalter, <https://perma.cc/6TU9-4CCH>; "Notice and Cure Provisions", *Canna Law Blog* (Dec. 26, 2021), <https://harris-sliwoski.com/cannalawblog/notice-and-cure-provisions/>.

[143] Shaleen Khanal, Hongzhou Zhang & Araz Taeihagh, "Why and How Is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI" (2025) 44 Policy and Society 52 (discussing how companies like Alphabet (Google), Amazon, Apple, Meta, and similar tech conglomerates not only lead in AI development but also own or manage key digital platforms and distribution ecosystems critical for monetising generative outputs.).

[144] Lina M Khan, "Amazon's Antitrust Paradox" (2017) 126 Yale LJ 710 at 744–752 (arguing that dominant digital platforms consolidate power by controlling infrastructure, user data, and downstream access); Daryl Lim, "Antitrust's AI Revolution" (2022), 89 Tenn L Rev 679 at 681 ("Dominant platforms compete directly with the businesses that depend on them while acting as gatekeepers for billions of dollars in economic activity. With more companies relying on fewer digital platforms to trade, antitrust law's ability to address "killer acquisitions," the exercise of intellectual property rights, access to vaccines during the COVID-19 pandemic, and even more traditional sectors of the economy will impact us for decades to come"); Daryl Lim & Peter K. Yu, "The Antitrust-Copyright Interface in the Age of Generative Artificial Intelligence" (2025) 74 Emory LJ 847 at 857-861 (discussing antitrust enforcement of big tech).

of identity-linked data may find themselves constrained not only by legal ambiguity but also by their dependence on the very platforms that facilitated the harm. Moreover, platform gatekeeping over content moderation and access to developer tools can influence whether and how redress mechanisms, such as takedown processes or identity verification tools, are made available.[145] While this Article focuses on intellectual property and data governance, these dynamics point to the need for complementary interventions in antitrust law and platform accountability.

5. *Limited Excludability*

The data right would not grant blanket exclusivity over identity-related data. Instead, it focuses on high-fidelity proxies, such as AI-generated voice clones, photorealistic avatars, or emulated performances, where the risk of deception, reputational harm, or misappropriation is real and narrowly defined. General characteristics, like broad artistic style, facial features shared across populations, or widely available speech patterns would remain outside its scope. By narrowly targeting the kinds of uses most likely to cause harm while preserving access to general data and public discourse, this design ensures that the right protects dignity and autonomy without stifling innovation, satire, or scientific progress.

This calibrated structure responds to a longstanding critique of overbroad publicity and privacy claims that risk privatising the cultural commons.[146] Courts have traditionally resisted attempts to monopolise generalised features, like a person's "style", aesthetic, or catchphrases, in the absence of strong identifying markers.[147] The proposed data right follows this tradition by requiring a demonstrable link between the AI-generated output and the individual's distinct, recognisable identity. This threshold requirement serves as a doctrinal gatekeeper, filtering out speculative or tenuous claims.

The emphasis on high-fidelity proxies is grounded in empirical reality. Advances in generative AI have made it increasingly difficult for audiences to distinguish real from synthetic content, especially when such outputs convincingly mimic a specific voice, likeness, or gesture.[148] The legal risk arises not merely from the copying of abstract traits, but from the production of digital doubles that audiences plausibly mistake for the real person.[149] Such synthetic impersonations are precisely where consent, accountability, and redress are most urgently needed.

---

[145] Niva Elkin-Koren et al., "Social Media As Contractual Networks: A Bottom Up Check on Content Moderation", (2022), 107 Iowa L Rev 987 at 1007 ("Platforms possess largely unrestrained discretionary power in content moderation, which may carry serious implications for individual creators, speakers, subscribers, and the public at large.").

[146] *Supra* note 71.

[147] *ETW Corp. v. Jireh Publ'g, Inc.*, 332 F.3d 915 at 938 (6th Cir., 2003) (finding that a general "style" or "persona" cannot be exclusively appropriated under right of publicity claims).

[148] Nils C Köbis, Barbora Doležalová & Ivan Soraperra, "Fooled Twice: People Cannot Detect Deepfakes but Think They Can", (2021), 6 iScience, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8602050>, (finding participants perceived AI-generated voices as matching the real speaker's identity approximately 80% of the time and could identify them as synthetic only about 60% of the time).

[149] U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law, "Hearing on the NO FAKES Act" (Nov. 2023), <https://www.judiciary.senate.gov/committee-activity/hearings/the-no-fakes-act-protecting-americans-from-unauthorized-digital-replicas>.

Limiting protection to identity-sensitive proxies also aligns the data right with free expression values. Parodic and transformative applications, such as a humorous spoof or academic text mining of publicly available videos, would remain unencumbered. This balance mirrors existing doctrines that exclude standard or unoriginal elements and the fair use doctrine, which protects critical, educational and non-substitutive reuses.[150] A data right tailored to specific risks avoids the chilling effects that could arise from vague or overly expansive protections.

Internationally, the proposed approach resonates with initiatives such as Denmark's likeness-as-copyright proposal, which similarly restricts protection to realistic digital simulations that could be mistaken for the individual.[151] Denmark's draft law, introduced in June 2025, would give individuals legal rights over the use of their face, voice, and other personal attributes in AI-generated content. It empowers citizens to demand removal of unauthorised deepfakes and imposes substantial penalties on platforms that fail to comply. The law distinguishes between deceptive digital impersonations and protected forms of expression such as parody and satire, thereby balancing individual dignity with freedom of speech.

The data right this Article proposes maintains fidelity to foundational legal principles, such as notice, proportionality, and harm-based thresholds, while adapting them to a technological landscape where imitation at scale has become trivial. It acknowledges that not all data use is equally invasive or consequential, and that regulatory responses should be calibrated accordingly. By anchoring liability in factors like identifiability, material impact, and the presence or absence of consent, the regime avoids sweeping prohibitions that could chill innovation or suppress expression.

C. *Implementation*

The proposed data right would be enacted through US federal legislation, setting a national baseline while preserving states' ability to adopt stronger protections. Enforcement would follow a layered approach: The approach would consist of the following: (1) Federal agency enforcement, (2) Private right of action, (3) Technical safeguards, and (4) Scaled compliance burdens and de minimis exemptions.

1. *Federal Agency Enforcement*

The FTC would serve as the primary public enforcer of the proposed data right, issuing rules, conducting audits, and investigating violations. Its longstanding expertise in data privacy, consumer protection, and deceptive trade practices makes it uniquely positioned to regulate identity-linked harms in the AI era.[152] Its existing

---

[150] *Campbell v. Acuff-Rose Music, Inc.*, (1994) 510 U.S. 569; *Authors Guild v. Google, Inc.*, 804 F.3d 168 (2d Cir., 2015); *Dr Seuss Enterprises LP v. ComicMix LLC*, 983 F.3d 443 (9th Cir., 2020); *Andy Warhol Foundation for the Visual Arts v. Goldsmith*, (2023), 598 U.S. 508; *Keck v. Mix Creative Learning Center LLC*, 116 F.4th 448 (5th Cir., 2024).

[151] Amelia Nierenberg, "Denmark Aims to Use Copyright Law to Protect People from Deepfakes", *The New York Times* (July 10, 2025), <https://www.nytimes.com/2025/07/10/world/europe/denmark-deepfake-copyright-ai-law.html>.

[152] Federal Trade Commission, "FTC Proposes New Protections to Combat AI Impersonation of Individuals" (Feb. 15, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals>.

mandate under Section 5 of the FTC Act which prohibits "unfair or deceptive acts or practices in or affecting commerce,"[153] provides a flexible and powerful legal foundation for addressing misuse of AI-generated likenesses, voice clones, and biometric simulations. Its enforcement authority would complement private lawsuits by setting industry-wide standards, assessing civil penalties, and providing regulatory oversight of companies' practices involving identity-linked data.

Unlike ad hoc litigation, FTC enforcement can establish *ex ante* norms through guidance, rulemaking, and policy statements.[154] The FTC's investigatory powers, ranging from civil subpoenas to consent decrees, are particularly well-suited to AI oversight. In recent years, the Commission has launched investigations into data brokers, biometric surveillance firms, and AI companies engaged in deceptive practices, often resulting in consent orders that require data deletion, algorithmic disgorgement, or compliance audits.[155] These remedies could be extended to companies that improperly train, deploy, or commercialise generative models using individuals' data without meaningful consent.

Moreover, situating public enforcement within the FTC leverages an existing institutional framework, avoiding the redundancy, delay, and resource demands that would accompany the creation of a new agency. It already houses technical experts in machine learning, data science, and privacy engineering, and maintains working relationships with global regulators through initiatives such as the Global Privacy Enforcement Network.[156] These attributes give the FTC both the substantive capacity and the jurisdictional reach to enforce the data right in a transnational and interoperable manner.

Finally, FTC oversight helps mitigate structural disparities in access to justice. Not all individuals harmed by AI-generated impersonations have the resources to bring suit, and many harms, especially dignitary or reputational ones, may go unaddressed in the absence of public enforcement. By creating a dual-track enforcement regime through private action and agency oversight, the data right maximises deterrence, reinforces norms, and expands coverage, all while remaining grounded in institutional pragmatism.

2. *Private Right of Action*

Individuals could pursue private lawsuits, with statutory damages and injunctive relief available, modelled after BIPA and CCPA. Statutory damages, like BIPA's $1,000 per negligent violation and $5,000 for wilful conduct help ensure that plaintiffs can seek redress even where harms are dignitary, reputational, or emotionally

---

[153] 15 U.S.C. 2024, (United States) § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

[154] Rohit Chopra & Lina M Khan, "The Case for "Unfair Methods of Competition" Rulemaking" (2020) 87 U Chicago L Rev 357.

[155] See *eg, re Everalbum, Inc.*, (Jan. 2021) (biometric data and facial recognition enforcement); *re Facebook, Inc.*, (July 2019) (privacy violations resulting in US$5 billion settlement).

[156] Federal Trade Commission, *Office of Technology*, <https://www.ftc.gov/about-ftc/bureaus-offices/office-technology>. See also Federal Trade Commission, "Multilateral Memorandum of Understanding for Participation in the "GPEN Alert" System", <https://www.ftc.gov/system/files/documents/cooperation_agreements/151026gpen-alert-mou.pdf>.

diffuse.[157] As in copyright law, these remedies alleviate the burden of quantifying actual economic loss in cases involving synthetic impersonation or unauthorised dataset inclusion.[158] Injunctive relief, similarly, would allow courts to halt the spread of AI-generated misuses and mandate deletion of unlawfully obtained identity-linked data.[159]

The CCPA underscores the importance of individual control over personal data but offers only limited recourse in the case of identity misappropriation by generative AI.[160] The proposed data right would fill this gap by targeting high-fidelity proxies of identity: like voice, likeness, biometric markers rather than general data misuse. Modelled in part on the NO FAKES Act, which creates a "digital replica right" and introduces consent-based safeguards rooted in publicity, privacy, and consumer protection law,[161] the proposed right expands this hybrid approach to include private enforcement, ensuring that individuals—not just states—can act to protect themselves.

By combining statutory damages, injunctive relief, and regulatory enforcement, the proposed framework delivers a pluralist enforcement model responsive to the unique characteristics of generative AI. It draws doctrinal legitimacy from existing IP, privacy, and consumer protection regimes while promoting interoperability with global frameworks that increasingly treat identity as both a data right and a personality interest.

3. *Technical Safeguards*

With the threat of federal enforcement and private action, the industry would be encouraged to adopt technical safeguards, such as watermarking, metadata tagging, and provenance tracking. These tools operationalise the data right by embedding accountability into the technological stack itself. Watermarking and metadata tagging enable creators, platforms, and regulators to identify the source and authenticity of AI-generated outputs, facilitating both detection and enforcement.[162] Provenance tracking helps establish whether identity-linked data was used without consent.[163] These mechanisms are already being advanced through initiatives like the Coalition for Content Provenance and Authenticity (C2PA), a cross-industry group co-founded by Adobe, Microsoft, the BBC, and others, which is developing open technical standards for content traceability and authenticity.[164] OpenAI has

---

[157] BIPA, *supra* note 26.

[158] *Douglas v. Cunningham*, (1935), 294 U.S. 207 at 210 (explaining that statutory damages were adopted to give copyright owners recompense for injury in situations where proving damages or profits is challenging despite proving infringement.).

[159] *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088 at 1095 (N.D. Ill., 2017).

[160] Cal. Civ. Code 2023 (United States, California) § 1798.150(a)(1).

[161] NO FAKES Act of 2023, S. 2890, 118th Cong., 2023 (United Sates); see also Transcript, U.S. Senate Judiciary Subcomm. on Intellectual Property, *NO FAKES Act Hearing* (Jan. 24, 2024), <https://www.techpolicy.press/transcript-us-senate-judiciary-subcommittee-hearing-on-the-no-fakes-act>.

[162] European Parliament, *Generative AI and Watermarking*, EPRS Briefing (2023) at 3 (noting that watermarking authenticates the origins and integrity of the content and enables tracing of outputs generated by AI systems).

[163] Shayne Longpre et al., "Data Authenticity, Consent, and Provenance for AI Are All Broken: What Will It Take to Fix Them?", *An MIT Exploration of Generative AI* (March 27, 2024), <https://mit-genai.pubpub.org/pub/uk7op8zs/release/2> (discussing the importance of data provenance, who needs it, and why.).

[164] Coalition for Content Provenance and Authenticity (C2PA), <https://c2pa.org>.

publicly stated its intention to include provenance signals and watermarking in its generative models,[165] while Google's SynthID tool embeds imperceptible watermarks directly into images generated by Imagen.[166] These technologies illustrate the feasibility of embedding accountability into generative systems without impairing output quality.

Regulatory design can accelerate adoption through a mix of carrots and sticks. Safe harbour provisions could shield developers or platforms from liability if they implement and adhere to certified safeguards. Certification schemes modelled after cybersecurity frameworks such as the National Institute of Standards and Technology's (NIST) AI Risk Management Framework[167] could provide reputational incentives and procurement eligibility. Public-sector procurement policies could further accelerate uptake by requiring watermarking or provenance compliance as a precondition for the use of generative AI systems in government services, thereby setting de facto market baselines.

This approach parallels the impact of the Digital Millennium Copyright Act (DMCA), which catalysed the development of automated notice-and-takedown systems, content recognition technologies, and platform accountability standards.[168] While the DMCA responded to the internet's disruption of copyright enforcement, a robust data right can similarly spur interoperable, verifiable safeguards for the AI age, complementing legal enforcement with technical due diligence and aligning with global trends toward embedded accountability.

A potential concern is that requiring robust provenance tools and audit capabilities may entrench the dominance of large platforms with the infrastructure to comply, thereby reinforcing existing asymmetries in the AI ecosystem.[169] To avoid privileging incumbents, the data right could be implemented alongside open-source compliance tools, shared verification frameworks, or public registries maintained by neutral bodies.[170] These measures would ensure that the burden of compliance does not deter entry or innovation among smaller developers, thereby aligning enforcement with the pluralist values the data right seeks to promote.

4. *Scaled Compliance Burdens and De Minimis Exemptions*

Small-scale and nonprofit users would benefit from scaled compliance burdens or de minimis exemptions. To preserve access to innovation and protect expressive

---

[165] OpenAI, *Our Approach to AI Safety*, <https://openai.com/safety>.

[166] Google DeepMind, *SynthID: Watermarking AI-Generated Images*, <https://deepmind.google/technologies/synthid/>.

[167] National Institute of Standards and Technology, "AI Risk Management Framework (AI RMF 1.0)", (2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

[168] Daryl Lim, "Notification and Permission-Based Approaches for Generative AI Platforms", (2024) *TechReg Chronicle* (discussing the DMCA's notice-and-takedown system in the context of AI regulation.).

[169] *Ibid*.

[170] Geoffrey A Manne et al., "Comments of the International Center for Law & Economics on the DOJ's "Promoting Competition in Artificial Intelligence" Workshop" (July 15, 2024), <https://laweconcenter.org/resources/icle-comments-to-doj-on-promoting-competition-in-artificial-intelligence/>, (arguing that supporting open-source development and shared tools enables non-incumbents to compete, preventing dominance by large firms that control infrastructure and distribution channels.).

freedom, the proposed data right would incorporate tiered obligations that adjust based on the size, purpose, and resources of the user. Individuals, startups, researchers, and nonprofits operating in good faith, particularly those without significant commercial intent, would face reduced administrative burdens or qualify for exemptions where the use of identity-linked data is minimal, incidental, or non-exploitative. This tiered model reflects principles already embedded in US intellectual property law.

For example, copyright law permits limited use of copyrighted material without prior authorisation in contexts such as commentary, criticism, education, and scholarship. Courts have routinely applied the fair use doctrine to protect nonprofit or educational users from liability where the use is transformative and serves the public interest.[171] Patent law offers reduced fees and simplified procedures for small and micro entities, acknowledging the importance of proportional compliance burdens.[172]

Similarly, the data right could incorporate a "research and education" safe harbour that permits identity-linked data use for socially beneficial applications, such as training models to detect algorithmic bias or studying cultural representations in AI-generated media, without triggering full compliance obligations. This would enable universities, libraries, and non-commercial developers to continue exploring responsible AI innovation without the fear of litigation or regulatory sanctions.

This design also aligns with modern regulatory frameworks that prioritise risk-based, proportionate governance. The EU AI Act, for instance, distinguishes between high-risk and low-risk AI systems and imposes graduated obligations accordingly.[173] A comparable structure in the data right would direct enforcement efforts toward large-scale commercial actors whose practices are most likely to result in reputational, emotional, or economic harm, such as deepfake distribution platforms or entertainment companies monetising synthetic likenesses. At the same time, it would affirm that protections for identity-linked data should not come at the expense of public-interest research, artistic experimentation, or democratic discourse.

In short, the data right offers a practical, pluralist governance solution for the identity-linked risks posed by AI. It strengthens individual agency, coordinates doctrinal fragmentation, positions the US to respond flexibly to future technological change, and serves as the connective tissue for a more resilient regulatory ecosystem. Together, these features make the data right not only a legal innovation but a necessary adaptation to the realities of a digitally mediated society.

V. Conclusion

A single AI-generated deepfake of Taylor Swift illustrates the central challenge of generative AI regulation: it implicates privacy, publicity, copyright and speech, yet

---

[171] *Authors Guild v. Google, Inc*., 804 F.3d 202 at 219–225 (2d Cir., 2015) (holding that Google Books' scanning of books for public search and scholarly use was fair use); see also *Campbell v. Acuff-Rose Music, Inc*., (1994), 510 U.S. 569 at 578–585 (discussing transformative use and nonprofit character as key fair use factors).

[172] 35 U.S.C. 2021 (United States) § 41(h); see also Manual of Patent Examining Procedure 9th edition Revision 01.2024 2024 (United States) § 509.02 (defining small and micro entities for fee purposes).

[173] EU AI Act, *supra* note 130, articles 6–7, 9, 51–52.

evades comprehensive redress under any single doctrine. This Article has argued that the overlapping and fragmented nature of these legal responses is not a structural flaw but a strategic virtue. Legal heterogeneity fosters adaptability, experimentation, and cross-pollination across doctrinal silos, an essential feature in responding to fast-moving technologies.

To build on this strength while addressing its limits, the Article proposes a narrowly tailored US federal data right. Designed to complement rather than displace existing frameworks, the right targets high-risk, identity-linked uses of data through consent-based, transparent, and enforceable rules. It addresses the accountability gap left by legacy doctrines, especially where identity is replicated at scale but legal protections remain partial or inapplicable. Such a solution is likely to be workable in jurisdictions that presently operate in a legally heterogeneous environment with a mélange of similar personality rights and intellectual property laws.

Rather than seeking premature harmonisation, the US can leverage its pluralistic system to incubate solutions responsive to evolving technological risks. A federal data right offers a path forward—one that is principled yet pragmatic, grounded in existing legal traditions yet capable of guiding future reform. By layering this right atop privacy, publicity, and copyright, and aligning with global trends, the US can forge a resilient regulatory ecosystem. Heterogeneity, properly structured, is not a hindrance but a feature—a democratic advantage in the age of generative AI.

* * *

Appendix: Comparative Legal Approaches to Regulating AI and Identity-Based Harms

Legal Doctrine	Primary Interest Protected	Trigger for Liability	Key Limitation	Conflict Risk	Reform Pathway
Privacy (Tort)	Dignitary harm, autonomy	Intrusion, disclosure, misappropriation	Requires individualized harm, state-by-state variation	May conflict with publicity when applied to public figures	Expand biometric statutes (eg, BIPA); harmonize with data rights
Right of Publicity	Commercial exploitation of identity	Unauthorized use of name, image, likeness in commerce	Fragmented; weak fair use protection	May conflict with copyright or be preempted by federal law	Federal statute (e.g., NO FAKES Act or ELVIS Act model)
Copyright	Original expression, creative labor	Substantial similarity; unauthorized copying of protected work	Excludes identity, style, or likeness unless fixed	May clash with publicity over expressive vs. factual uses	Dataset transparency; collective licensing; disclosure mandates
Proposed Data Right	Control over identity-linked data	Use of recognizable data in AI training/generation without consent	Still conceptual; unclear scope and defenses	Could overlap with or duplicate publicity and privacy claims	Opt-in consent; FTC rulemaking; safe harbors; private enforcement