THIS PROGRAM IS INTENDED FOR INFORMATIONAL PURPOSES ONLY. NOTHING SHOULD BE CONSTRUED OR TAKEN AS LEGAL ADVICE. 2026 ELI WRITING CONTEST ESSAY WRITTEN BY DEREK SONG.

From Voice Imitation to Data Exploitation: Reclaiming Musician Identity Through Biometric Privacy

I. Introduction

A musician's voice is their biological instrument: irreplaceable, immutable, and intimate. Artificial intelligence (AI) now treats that instrument as raw data to be mined and repurposed. When Hallwood Media signed Xania Monet, a fully AI-generated R&B artist using Suno (a generative AI music model), for $3 million,[1] the deal marked the crisis of artistic identity more than a triumph of innovation. Xania's music sounds like a chorus of human influences without belonging to any one of them.

The problem begins at ingestion, not imitation outputs. AI systems extract vocal characteristics from public recordings, model those attributes through machine learning, and encode those into systems capable of generating "new" synthetic vocals.[2] By the time the artists discover the use, their physiological data has already been captured, processed, and monetized.

Existing law does not offer an adequate remedy. Intellectual property and publicity doctrines regulate AI outputs with a focus on commercial exploitation and recognizable likeness. Consider musicians like Kehlani and SZA, who have publicly opposed AI-generated music,[3] yet lack legal standing unless they can prove the output "sounds like them." At that point, their voices have long been harvested and exploited. A solution which targets AI input, or the moment of data collection, provides a stronger incentive and clearer guidance for compliance.[4]

This paper argues for a federal consent-based biometric privacy framework that directly addresses this dignitary harm. Unconsented AI voice ingestion commodifies the biological aspects of performance. While publicity protects market value, biometric privacy protects personhood. The line between art and identity must hold even when new technologies try to erase the difference.

II. The Input Distinction and Right of Publicity's Structural Failure to Address AI Voice Harvesting

AI ingestion creates harms which the right of publicity cannot reach. When a company scrapes a musician's publicly available recordings to extract voiceprints for AI training, no commercial exploitation has occurred yet.[5] At ingestion, the musician's identity is not being

[1] Hannah Karp, *AI Artist Xania Monet Climbs the Charts — And Signs a Multimillion-Dollar Record Deal*, BILLBOARD (Sept. 16, 2025), https://www.billboard.com/pro/ai-music-artist-xania-monet-multimillion-dollar-record-deal/.

[2] *See* Peteris Asbahs, *How Does AI Voice Transformation Enhance Music Production?*, SONARWORKS BLOG (May 4, 2025), https://www.sonarworks.com/blog/learn/how-does-ai-voice-transformation-enhance-music-production; Amanda Downie & Molly Hayes, *What Is AI Voice?*, IBM THINK BLOG (May 2025), https://www.ibm.com/blog/what-is-ai-voice.

[3] Aria Bell, *Kehlani, SZA Slam AI Artist Xania Monet's Multimillion-Dollar Record Deal: "Children Are Dying"*, BLAVITY (Sept. 22, 2025), republished at *Yahoo! News*, https://www.yahoo.com/entertainment/music/articles/kehlani-sza-slam-ai-artist-203344886.html.

[4] Miriam H. Baer, *Governing Corporate Compliance*, 50 B.C. L. REV. 949, 956 (2009) (arguing that it may be "healthier" and more beneficial to "govern" corporate compliance, rather than to adjudicate it).

[5] Classic right of publicity cases address discrete, *public*-facing commercial appropriation. *See* Midler v. Ford Motor Co., 849 F.2d 460, 463 (9th Cir. 1988) (holding Ford liable for deliberately imitating Bette Midler's distinctive voice

publicly appropriated. But the harm is already done: the biometric data has been extracted, the voice model has been trained, and control has been lost. Right of publicity leaves a doctrinal void where unconsented ingestion of voice data goes unregulated. Even where commercial use eventually manifests, musicians face the compounding problems of jurisdictional chaos[6] from divergent state protections,[7] insurmountable proof barriers,[8] and First Amendment uncertainty.[9]

Traditional right of publicity cases addressed voice imitation by humans. Sound-alikes, impersonations, and digital re-creations were scrutinized for ad use or unauthorized sale. AI operates differently. Rather than imitating style, AI systems computationally profile physiology. Algorithms perform acoustic analysis measuring pitch patterns, vocal timbre, formant frequencies, spectral envelope characteristics, and melodic phrasing[10]—physiological qualities unique to Billie Eilish's whisper-singing or Freddie Mercury's operatic range. These measurements create a "voiceprint," or a biometric identifier as physiologically distinctive as a fingerprint. Once encoded into neural network parameters, the system can generate novel speech or singing the artist never performed. This extraction occurs invisibly during data scraping, without any public-facing signal. Xania Monet's synthetic voice exemplifies this invisibility.[11] Listeners cannot identify which specific artists' vocal data trained Monet's model, yet those source musicians receive neither credit nor compensation for the physiological data that enables her "performances." Under existing doctrine, musicians have no legal recourse in these cases.

This disconnect exposes right of publicity's structural limit. Rooted in misappropriation, the doctrine frames identity harms through trading on a likeness for profit.[12] Some court dicta

in broadcast commercial when the ad *aired*); *see also* Waits v. Frito-Lay, Inc., 978 F.2d 1093, 1099–1101 (9th Cir. 1992) (affirming liability attached to the act of *broadcasting* the sound-alike of Tom Waits in Doritos' radio ad).

[6] *See, e.g.*, Ettore v. Philco Television Broad. Corp., 229 F.2d 481, 485 (3d Cir. 1956) (describing the interstate broadcast choice-of-law problem as a "haystack in a hurricane"); Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 574–75 (1977) (recognizing the right of publicity but leaving the scope to state law); *see generally* Hart v. Elec. Arts, Inc., 717 F.3d 141, 153–63 (3d Cir. 2013) (surveying three competing balancing test for reconciling First Amendment with publicity rights).

[7] Andrews v. D'Souza, 696 F. Supp. 3d 1332 (N.D. Ga. 2023) (Georgia protects non-celebrity appropriation regardless of commercial value); *cf.* UTAH CODE § 45-3-1(1)(a) (limiting protection to personalities with commercial value).

[8] Cohen v. Facebook, Inc., 798 F. Supp. 2d 1090 (N.D. Cal. 2011) (dismissing misappropriation and Lanham Act claims where plaintiffs failed to allege cognizable injury or commercial interest in their names and likenesses).

[9] *Compare* Comedy III Prods., Inc. v. Gary Saderup, Inc., 25 Cal. 4th 387, 408–09 (2001) (finding drawings of literal Three Stooges depictions were not transformative when value was derived from plaintiffs' fame); *with* Winter v. DC Comics, 30 Cal. 4th 881, 890–92 (2003) (finding comic book characters based on Johnny and Edgar Winter were clearly transformative for adding fanciful and creative elements beyond likeness); *and* Kirby v. Sega of Am., Inc., 144 Cal. App. 4th 47, 58–60 (Ct. App. 2006) (narrowly holding a video game character was transformative due to anime styling and futuristic context).

[10] *See generally* Anil Pudasaini et al., *A Comprehensive Study of Audio Profiling: Methods, Applications, Challenges, and Future Directions*, 640 NEUROCOMPUTING 130334, 2–5 (2025).

[11] *See* Karp, *supra* note 1.

[12] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 403 (1960) (noting that the tort of appropriation as a privacy right is virtually indistinguishable from the right of publicity); Brooks v. Thomson Reuters Corp., No. 21-cv-01418-EMC, 2021 WL 3621837, at *2–3 (N.D. Cal. Aug. 16, 2021) (recognizing California's right of publicity as a "commercial misappropriation" claim and analyzing identity harms through the appropriation framework).

have even conflated the tort of appropriation and publicity law as substantively identical.[13] But AI voice extraction is data exploitation, not appropriation. The AI company does not use the musician's voice to sell products or trade on celebrity association.[14] Instead, the company benefits from computationally processing the biometric data itself—to enable realistic speech synthesis derived from vocal patterns.[15] Injury is better classified as privacy-informational rather than reputational or purely financial. Scholars have cautioned that folding these privacy-based harms back into publicity collapses the boundary between the individual and the commercial entity,[16] eroding doctrinal clarity.

Biometric privacy law directly targets this distinct dignitary harm. As the Seventh Circuit explained, "noncompliant collection of biometric data amounts to an invasion of an individual's private domain, much like an act of trespass."[17] Unlike publicity, liability for harm anchors at collection, irrespective of later use. This framework recognizes informational self-determination, or control over sensitive biological identifiers. For musicians, streaming a song authorizes consumption of the artistic work, not extraction of vocal anatomy for machine learning. A biometric privacy framework addresses ingestion-stage harm by protecting informational privacy upstream while preserving downstream commercialization under publicity.

Within the intellectual property ecosystem, each doctrine has a clear locus: copyright law protects output expression, patent law protects the technological process, and right of publicity protects commercial persona. Biometric privacy protects physiological information. These are complementary frameworks. Expanding publicity to cover data would distort its economic purpose; creating a separate biometric framework preserves doctrinal clarity.

This biometric framework already exists in practice. Illinois's Biometric Information Privacy Act (BIPA) shows how informed consent can operate as the controlling safeguard for identity in data-driven contexts. Its treatment of voiceprints provides a concrete framework for regulating AI voice ingestion without stretching IP or publicity law beyond recognition.

III. The Privacy Law Framework and the Feasibility of Regulating Voiceprints as Biometric Identifiers

[13] Somerson v. World Wrestling Ent., Inc., 956 F. Supp. 2d 1360, 1365 (N.D. Ga. 2013) ("…there is *no substantive difference* between the interests protected by the common law 'right of privacy' and the interests protected by the appropriation prong of the invasion of privacy tort…").

[14] Jacob Gaba, *Can Someone Own a Voice? Breaking Down the Right of Publicity*, FIRE (Aug. 1, 2024), https://www.thefire.org/news/can-someone-own-voice-breaking-down-right-publicity ("Rather, Sky's value lies in the actual service provided, that is, the voice's ability to interact with users. Sky would possess that value regardless of whether it sounded like [Scarlet] Johansson or not.").

[15] Robert Hart, *Here's Why Other Celebrities Could Face Problems With AI Voice Cloning—Not Just Scarlett Johansson*, FORBES (May 24, 2024), https://www.forbes.com/sites/roberthart/2024/05/24/heres-why-other-celebrities-could-face-problems-with-ai-voice-cloning-not-just-scarlett-johansson (finding that AI voice imitation primarily stems from a broader technological drive toward realism rather than individualized exploitation).

[16] Lisa Raimondi, *Biometric Data Regulation and the Right of Publicity: Protecting Identity in the Age of Artificial Intelligence*, 16 U. MASS. L. REV. 198, 218–19 (2021); Jennifer E. Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* 137 (Harvard Univ. Press 2018).

[17] Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1162 (7th Cir. 2021) (quoting Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 624 (7th Cir. 2020)).

A. Illinois BIPA's Consent-Based Framework for Voice Biometrics

BIPA establishes a consent-based framework for the collection and use of biometric data. BIPA defines "biometric identifier" to include "voiceprints" and prohibits unauthorized collection, retention, and use.[18] Its protections extend to the loss of the right to control one's biometric information. By regulating the extraction of voice characteristics regardless of source, function, or downstream application, BIPA's operative safeguard is "informed consent" rather than a categorical ban. [19]

Illinois courts have consistently interpreted this consent requirement broadly. In *Rosenbach v. Six Flags*, the Illinois Supreme Court held that BIPA violations occur upon noncompliance with *any* one of BIPA § 15's requirements, regardless of actual injury.[20] Six Flags' failure to notify or obtain the consent of a minor and his parent before fingerprint collection constituted a technical violation.[21] That technical violation created "aggrieved" standing within the statute's meaning at the moment of *collection*.[22]

Rosenbach's reasoning has since been extended to voice data. In *Wilcosky v. Amazon*, the Northern District of Illinois found Article III standing under both §§ 15(b) and 15(a).[23] Plaintiffs alleged Amazon's Alexa retained voice profiles indefinitely without notice or consent.[24] The court held that this indefinite retention and processing of voiceprints constituted concrete injury, even absent commercial use or identification.[25] A year later, *Carpenter v. McDonald's Corp.* reaffirmed and expanded this reasoning. [26] There, plaintiffs alleged McDonald's AI drive-through system collected customer voiceprints without prior consent in violation of § 15(b).[27] Critically, the court rejected McDonald's argument that BIPA requires actual use of a voiceprint for identification,[28] finding the violation complete if the collected data *could* identify an individual.[29] Notably, *Carpenter* made no distinction based on voluntary engagement with the AI assistant, underscoring that participation alone does not substitute for informed consent.[30] The court's silence on voluntariness reinforces BIPA's categorical focus on the act of collection. Together, these decisions illustrate how BIPA's consent-based regime squarely governs AI-driven voice analysis and leaves no room for "implied consent."

Collectively, Illinois courts have interpreted BIPA to recognize privacy violations as dignitary harms that occur at the moment of unconsented capture. This injury implicates

[18] 740 ILL. COMP. STAT. 14/10.

[19] 740 ILCS 14/15.

[20] *See* Rosenbach v. Six Flags Entm't Corp., 2019 Ill 123186, ¶ 33.

[21] *Id.* at ¶¶ 5–8.

[22] *Id.* at ¶¶ 33–34.

[23] Wilcosky v. Amazon.com, Inc., 517 F. Supp. 3d 751, 761–62 (N.D. Ill. 2021).

[24] *Id.*

[25] *Id.*

[26] Carpenter v. McDonald's Corp., 580 F. Supp. 3d 512 (N.D. Ill. 2022).

[27] *Id.*

[28] *Id.* at 518 n.2 (*emphasis added*) ("The collection of a voiceprint—which is explicitly included in the definition of 'biometric identifier'—without consent, even if not collected for the purpose of identifying that person, is a violation of the statute.").

[29] *Id.* at 518.

[30] *Id.* at 519–20.

autonomy and informational control rather than economic loss. The logic applies naturally to musicians, especially singers: when a singer cuts a track, they authorize public listening. AI training that scrapes recordings to build "new performances" the artist never agreed to give or would compromise the artist's vocal anatomy transforms participation into exploitation. The harm shifts from lost profits to lost agency. As *Rosenbach* confirmed, liability arises from noncompliance with consent requirements, regardless of quantifiable financial damages.[31] Unlike the right of publicity's safeguarding market value, BIPA safeguards the right to decide whether one's biometric data is captured at all. That autonomy interest endures even where a famous musician has voluntarily placed aspects of their voice or image in the public domain. Exposure does not exhaust their right to refuse biometric extraction. Public dissemination may market the art but does not waive control over personhood.

B. Public Distribution Does Not Waive Biometric Privacy Rights

Musicians commercialize their performances by distributing recordings publicly. But public exposure is not permission. Dissemination is indeed an expansion of access but does not per se totally dissolve control. Courts have rejected the notion that public dissemination waives biometric privacy.

In *In re Clearview AI*, the Northern District of Illinois outright rejects the argument that BIPA excludes biometric data derived from publicly available photographs.[32] The court explains a biometric identifier is "not the underlying medium."[33] Instead, the court considers if physiological measurements used to identify a person have been collected—expressly listing *voice* alongside face, finger, and eye as physiological measurements.[34] Therefore, public accessibility does not waive biometric privacy rights. It is the act of extraction that triggers statutory liability.

Although the Ninth Circuit in *Patel v. Facebook* was applying Illinois's BIPA, its reasoning reflects federal appellate confirmation that Illinois's interpretation of biometric privacy is sound.[35] The court held that Facebook's creation and retention of facial templates from user-uploaded photos without consent violated BIPA.[36] The court emphasized that the violation stemmed from the unconsented collection and storage of biometric data itself.[37] Relying on the Supreme Court's reasoning in *Spokeo, Inc. v. Robins*, the Ninth Circuit recognized that an invasion of biometric privacy rights constituted a concrete injury "[closely related] to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[38] Notably, *Patel* does not discuss public accessibility of the underlying Facebook photos. The omission suggests that publicity status was immaterial to BIPA's consent analysis.

[31] *Rosenbach*, 2019 Ill 123186 at ¶ 33.

[32] In re Clearview AI, Inc., Consumer Privacy Litig., 585 F. Supp. 3d 1111, 1123 (N.D. Ill. 2022).

[33] *Id.* (quoting Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017)).

[34] *Id.*

[35] Patel v. Facebook, Inc., 932 F.3d 1264, 1268, 1271–73 (9th Cir 2019).

[36] *Id.*

[37] *Id.*

[38] *See id.* at 1273 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).

The idea that publicity is immaterial to the consent analysis is increasingly reflected in legislation. Texas's Capture or Use of Biometric Identifier Act ("CUBI"),[39] as amended by the Texas Responsible Artificial Intelligence Governance Act ("TRAIGA"),[40] expressly rejects the theory that publicity equates to consent. TRAIGA clarifies that an individual does not consent to the collection of biometric data merely because media containing that data is publicly available.[41] The statute reflects consensus that biometric control persists beyond exposure.[42]

Altogether, case law and statutory developments map an emerging doctrine that the right to control biometric identity survives publication. For the music industry, this is decisive. A musician releasing a recording does not authorize third parties to extract and algorithmically reproduce their voiceprint any more than an Instagram selfie authorizes facial geometry scraping.

C. Biometric Privacy Law Should Be Federalized

State biometric laws prove the framework's viability but expose its limits. Illinois protects voiceprints without exception. Washington, by contrast, excludes "data generated from…audio recording" from its biometric identifier.[43] This leaves vocal data uncovered despite listing "voiceprint."[44] Texas offers comparable protections to BIPA but, like Washington, limits enforcement to the attorney general.[45]

This fragmentation produces jurisdictional incoherence. Imagine a singer whose voice is scraped from Spotify by an AI music generation lab. An artist in Illinois can sue directly; in Texas, they must depend on attorney general enforcement; in Washington, no remedy exists. Yet the underlying harm from computational voice extraction remains the same. Accordingly, state variation demonstrates the need for federal harmonization.

IV. The Viability of a Federal Biometric Privacy Framework as a Doctrinally Coherent Solution

D. Constitutional Grounding and Comparable Statutory Authority

[39] TEX. BUS. & COM. CODE ANN. § 503.001 (West, Westlaw through 2025 Reg. Sess.) (amended by Act of May 24, 2025, 89th Leg., R.S., ch. 1174, § 2, eff. Jan. 1, 2026).

[40] TEX. GOV'T CODE ANN. §§ 551.053–.057 (West, Westlaw through 2025 Reg. Sess.) (added by Act of May 24, 2025, 89th Leg., R.S., ch. 1174, § 1, eff. Jan. 1, 2026) (creating exceptions only for security-related systems).

[41] TRAIGA, TEX. GOV'T CODE ANN. §§ 551.053–.057; *see also* Amanda Witt & Jennie Cunningham, *Texas Legislature Passes House Bill 149 to Regulate AI Use*, Nelson Mullins (June 12, 2025), https://www.nelsonmullins.com/insights/alerts/privacy_and_data_security_alert/all/texas-legislature-passes-house-bill-149-to-regulate-ai-use (summarizing TRAIGA and its implications on biometric collection).

[42] *Id.*

[43] BI, WASH. REV. CODE § 19.375.010 (2020).

[44] *Id.*

[45] To date, there have only been two notable enforcement actions by the Texas attorney general and none under Washington's biometric statute. See *Texas Biometrics Case Highlights Need for Consent: Meta Settles for $1.4 Billion*, V&E Data Privacy Update (Aug. 5, 2024), https://www.velaw.com/insights/texas-biometrics-case-highlights-need-for-consent-meta-settles-for-1-4-billion/ (reporting $1.4 billion settlement with Meta under the Texas Capture or Use of Biometric Identifier Act and related privacy laws); see also Press Release, Office of the Att'y Gen. of Tex., *Attorney General Ken Paxton Secures Historic $1.375 Billion Settlement with Google Related to Texans' Data Privacy Rights* (May 9, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-historic-1375-billion-settlement-google-related-texans-data.

Congress has clear constitutional authority to enact a federal biometric privacy statute. AI training and dissemination are inherently interstate commerce where data transmission centers and model deployment span multi-state jurisdictions. Under Commerce Clause precedent, a National Biometric Information Privacy Act would easily satisfy constitutional thresholds for regulating interstate AI training.[46] In fact, a version was proposed in 2020 but failed beyond committee review, confirming both feasibility and congressional awareness of this existing issue.[47]

Federal privacy frameworks already exist (HIPAA, COPPA, FCRA), each employing consent mechanisms proportional to data sensitivity.[48] Common to all of these statutes is the theory that the more immutable and personally identifying the data, the stronger the protection. Biometric identifiers are comparably, if not more, immutable and personally identifying.[49]

The main constitutional tension arises under the First Amendment. But even these concerns are limited. As discussed earlier, biometric privacy law regulates collection *conduct* rather than expressive *content*. Requiring informed consent prior to data collection, storage, and processing does not suppress speech. A consent and disclosure framework is narrowly tailored to establish conditional access for highly sensitive personal information. Courts have consistently upheld similar consent and disclosure rules in comparable commercial contexts.[50] Narrowly governing the point of data capture as a matter of procedure sidesteps the substantive expressive use challenges that publicity law faces.

In short, federal biometric privacy fits comfortably within congressional authority and established consent frameworks. The next inquiry evaluates whether existing publicity law could fill this role or whether a distinct statutory right remains necessary.

E. The Right of Publicity Cannot Substitute for Biometric Privacy

Recent litigation illustrates the right of publicity's persistent limitation to output-stage harms. In *Lehrman v. Lovo*, the Southern District of New York allowed publicity claims under New York Civil Rights law §§ 50 – 51 to survive a motion to dismiss where voice actors contested unauthorized use of their AI-cloned voices in marketing material and consumer offerings.[51] Here, the court interprets "digital replicas" to encompass synthetic voices that were

[46] U.S. CONST. art. I, § 8, cl. 3; Gonzales v. Raich, 545 U.S. 1, 17 (2005) (holding Congressional authority extends to local activity which has a substantial interstate effect); Wickard v. Filburn, 317 U.S. 111, 125 (1942) (same).
[47] National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020).
[48] Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d–1320d-9; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x.
[49] Müge Fazlioglu, *U.S. Data Privacy Litigation: Biometrics and Consumer Health Data*, INT'L ASS'N OF PRIV. PROFS. (Mar. 2025), https://iapp.org/resources/article/us-litigation-series-biometrics-consumer-health-data/.
[50] *See, e.g,* Zauderer v. Office of Disciplinary Counsel, 471 U.S. 626, 651 (1985) (finding disclosure requirements trench more narrowly on an advertiser's interests than flat speech prohibitions); *see also* Trans Union LLC v. FTC, 295 F.3d 42, 53 (D.C. Cir. 2002) (holding that FTC's GLBA privacy rules requiring notice and limit reuse of consumer financial data regulated speech to protect privacy interests within the appropriate constitutional limits); Sorrell v. IMS Health Inc., 564 U.S. 552, 577–78 (2011) (recognizing privacy as a substantial state interest and noting that content-neutral consent or disclosure regimes would be permissible under the First Amendment).
[51] Lehrman v. Lovo, Inc., No. 24-CV-3770 (JPO), 2025 WL 1902547, *20–24 (S.D.N.Y. July 10, 2025).

perceptibly identical to the plaintiffs' voices.[52] But the court stops at deployment. *Lehrman* makes no finding regarding the training process by which Lovo extracted voice characteristics. Implicit in *Lehrman* is publicity's continuing structural constraint in governing display, not data. The logic applies equally to vocalists: publicity law addresses the unauthorized output performance but not the upstream clone-enabling data. In reality, the act of harvesting biometric data to train a replicant is comparably, if not more, invasive than its later commercial use.[53]

Statutory reform has also failed to close this gap. Tennessee's 2024 ELVIS Act and the proposed federal NO FAKES Act each prohibit the unauthorized "use," "publication," or "distribution" of synthetic AI in expressive works or advertisements.[54] Both of these statutes aggressively expand output protection with express protections against public dissemination of digital replicas.[55] Nonetheless, both statutes are insufficient as a legal or regulatory incentive for an AI company to engage in proactive compliance. Professor Rothman notes, the revised No FAKES Act actually "[undoes] some of the protections provided in the Take It Down Act" by allowing "broad licenses and authorized representatives to permit the dissemination of [AI-generated] intimate images" without specific consent.[56]

Renewing or expanding publicity doctrines only replicates structural deficiencies and floods the court with fact-intensive litigation. A more coherent solution is to move away from commerciality and toward the initial act of data ingestion, shifting protection upstream. This supports operationalizing a consent-based framework within AI systems themselves.

F. Practical Implementation of an Opt-in Consent-Based Mechanism in AI Systems

Covered entities would include AI music generation platforms, streaming services providing data to third parties, and any entity extracting voiceprints from recordings for model training. Before any ingestion, explicit and informed consent must be obtained from the artist or rightsholder. Consent disclosures should specify: 1) the nature of the biometric data collected; 2) the purpose and scope of use; 3) retention and deletion timelines; and 4) any intended sharing or transfer of that data. These procedural requirements are based on BIPA requirements[57] and match existing federal frameworks[58]—they are minimally intrusive and compatible with AI developers' existing data governance protocols.[59]

[52] *Id.* at *23.

[53] *See* Andrew Park, Jan Kietzmann & Jay Killoran, *The Risks of Collecting Employees' Biometric Data*, HARV. BUS. REV. (May 29, 2025), https://hbr.org/2025/05/the-risks-of-collecting-employees-biometric-data (finding that biometric data collection, even without misuse, creates significant feelings of insecurity, loss of autonomy, and psychological harm among employees in the corporate workplace context).

[54] ELVIS Act, 2024 Tenn. Pub. Acts 842; NO FAKES Act of 2024, S. 2933, 118th Cong.

[55] *Id.*

[56] *See* Jennifer E. Rothman, *Reintroduced No FAKES Act Still Needs Revision*, Reg. Rev. (Aug. 18, 2025), https://www.theregreview.org/2025/08/18/rothman-reintroduced-no-fakes-act-still-needs-revision/.

[57] 740 ILCS 14/15(b).

[58] *See* HIPAA, COPPA, and FCRA, *supra* note 48.

[59] *See, e.g., OneTrust Unveils New Data Governance Solution to Close the Enforcement Gap for AI-Ready Data,* OneTrust (May 8, 2025) (press release), https://www.onetrust.com/news/onetrust-unveils-new-data-governance-solution-to-close-the-enforcement-gap-for-ai-ready-data/ (illustrating feasibility of consent-based data-use enforcement in AI systems); *see also Data Ethics in AI: 6 Key Principles for Responsible Machine Learning*,

Enforcement should provide a private right of action,[60] statutory damages per violation without aggregate caps,[61] and no proof of actual economic harm requirement. Plaintiffs should retain the option to elect actual damages where provable pecuniary losses exceed statutory amounts.[62] In turn, compliant entities should qualify for safe harbor protection. This framework balances deterrence and efficiency, creating meaningful incentives for proactive data governance instead of reactive litigation. It aligns incentives among data subjects, rightsholders, and AI developers, ensuring regulatory certainty without chilling innovation.[63]

Adopting BIPA's narrow exceptions, bona fide research subject to institutional review, law enforcement pursuant to warrants, or defined security functions to prevent fraud or unauthorized access are excluded.[64] Still, unconsented biometric extraction for commercial AI training would be expressly prohibited. Retention limits must require destruction of biometric data once the stated purpose expires or upon the subject's request. Technical infeasibility of complete "untraining" does not excuse retention or continued model deployment.[65] If removal is computationally impractical, commercial use of that data-derived model must be prohibited. This ensures accountability even where current unlearning limitations in neural networks shift balancing costs.[66]

Industry practice and leadership statements further support the viability of an opt-in consent mechanism. Sam Altman has announced plans to implement opt-in consent for copyright

Alation (July 15, 2024), https://www.alation.com/blog/data-ethics-in-ai-6-key-principles-for-responsible-machine-learning/ (noting industry awareness of consent as a recurring ethical consideration in AI data governance).

[60] While Texas attorney general enforcement has yielded billion-dollar settlements, *see* supra note 45, jurisdictions that rely exclusively on state attorney general action remain largely under-litigated. A private right of action ensures that individual musicians can seek redress independent of state enforcement priorities.

[61] *See* 740 ILCS 14/20 (2024); Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 927–29 (Ill. 2023) (holding that a new claim accrues each time biometric data is captured or disclosed without consent). For voiceprints, each extraction of voice data—including scraping recordings, accessing multiple platforms, or updating AI training datasets—should constitute a separate violation. Musicians with substantial catalogues and higher propensity for extraction can recover mass amounts through cumulative violations. Illinois now has limited aggregate recovery, 2024 Ill. Legis. Serv. P.A. 103-0769, but a federal framework should preserve *Cothron* per-violation accountability for AI voice extraction, given the AI's capacity for mass, automated misuse. Courts retain authority to ensure proportionality in exceptional cases. *See* State Farm Mut. Auto. Ins. Co. v. Campbell, 538 U.S. 408, 426 (2003).

[62] 740 ILCS 14/20 (2024) (plaintiffs may recover the greater liquidated damages or actual damages). Federal privacy law's limitation of "actual damages" to proven pecuniary loss, *FAA v. Cooper*, 566 U.S. 284, 300–01 (2012), does not constrain biometric voice protection. Statutory damages redress the dignitary harm of unconsented collection rather than economic loss. The per-violation framework, *see supra* note 61, ensures that consent violations remain actionable without proof of financial injury, preserving biometric privacy as a gatekeeping right.

[63] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1919–20 (2013) (Professor Julie Cohen explains, "[i]nnovative practice is threatened most directly when circumstances impose intellectual regimentation." Privacy, she adds, safeguards the "breathing room" that makes innovation possible, ensuring that creative practice can develop free from the chilling effects of pervasive monitoring and behavioral modulation.)

[64] *See generally* 740 ILCS 14/10 (enumerating exceptions to collection prohibitions); *General Data Protection Regulation* (GDPR), Regulation (EU) 2016/679, 2016 O.J. (L 119) 1, art. 9(2).

[65] *See* Alkis Koudounas et al., *"Alexa, Can You Forget Me?" Machine Unlearning Benchmark in Spoken Language Understanding* (May 21, 2025) (preprint), https://arxiv.org/abs/2505.15700.

[66] *Id.*

holders in training its Sora 2 video generation model.[67] This implies that implementing an opt-in system and large-scale consent tracking is technologically and administratively workable. The remaining gap is public relations[68] and legal compulsion. A federal biometric privacy statute would convert voluntary compliance into binding duty, ensuring that consent to create remains as meaningful as consent to perform.

V. Conclusion

AI voice extraction transforms a musician's unique physiology into raw data, severing identity from embodiment. Courts interpreting BIPA have held that capturing a voiceprint without consent violates privacy, irrespective of downstream use. Musicians should receive the same protection nationwide. A federal biometric privacy framework provides clarity through informed consent, statutory damages, and private enforcement. The technology is here; what remains is congressional action. From emerging artists protecting their first recordings to legacy catalogs of deceased legends, biometric privacy ensures that consent to share music is never mistaken for consent to surrender voice.

[67] Anthony Ha, *Sam Altman Says Sora Will Add "Granular," Opt-In Copyright Controls*, TECHCRUNCH (Oct. 4, 2025, 9:26 AM PDT), https://techcrunch.com/2025/10/04/sam-altman-says-sora-will-add-granular-opt-in-copyright-controls/.
[68] *Id.*