

NOTE

EX ANTE, EX POST, OR A COMBO OF BOTH? A COMPARATIVE ANALYSIS OF BIOMETRIC ARTIFICIAL INTELLIGENCE ACROSS THE ATLANTIC & THE SELF- REGULATORY SOLUTION

Ariana Tagavi*

Every second of the day, a face scan unlocks a smartphone, allows a traveler to pass through airport security, or signs an employee into a workplace attendance system. Now, more than ever, these same biometric inputs also power artificial intelligence (AI) systems that infer, predict, and categorize human behavior. Yet, these technologies that promise frictionless identity authentication and enhanced security have generated billions of dollars in litigation in the United States alone and triggered regulatory scrutiny around the world.

Biometric systems, now deeply integrated with AI, have become a focal point for competing visions of digital governance. The European Union has adopted an ex-ante, rights-protective regulatory model that seeks to constrain high-risk AI uses before they even enter the market. The United States, by contrast, relies largely on an ex-post, liability-driven approach characterized by fragmented statutes and private litigation. Both frameworks reflect distinct constitutional traditions and regulatory philosophies, yet, both reveal limitations when applied to rapidly evolving biometric-AI systems.

This Note examines how these two dominant regulatory traditions shape the governance of biometric technologies and

* Ariana Tagavi J.D. Candidate, 2026, Fordham University School of Law, *Fordham International Law Journal* Executive Symposium Editor; B.A. in International Studies and Spanish Language, Literature, and Culture, 2021, University of Michigan. I extend my sincere gratitude to Professor Caroline Gentile for her profound impact and guidance throughout my law school career, especially in pursuit of this Note. Thank you also to the *Fordham International Law Journal* 2025–2026 and 2026–2027 editors and staff for all their hard work.

assesses whether a structured self-regulatory organization (SRO) could address the shortcomings inherent in both. It proceeds in three parts. Part I defines biometric data in the AI era and maps three governance architectures: (1) the EU's rule-bound, precautionary model; (2) the United States' enforcement-oriented regime; and (3) industry-led SRO analogies that operationalize technical and procedural safeguards through existing hard law and soft law frameworks and a hypothetical biometric AI version. Part II presents a comparative analysis of these regimes, examining how each addresses the core challenges of biometric-AI risks, including the protection of individual rights, incentives for innovation, and the effectiveness of enforcement mechanisms. Part III advances a structured SRO framework, arguing that a formally constituted, standards-driven body could provide the flexibility, technical expertise, and ongoing oversight that neither purely statutory regulation nor litigation-based enforcement currently offers.

I.UNDERSTANDING THE WORLD OF BIOMETRIC AI	
GOVERNANCE	1472
A. Defining Biometric Data and Its Relationship with Artificial Intelligence	1472
B. Description of the Three Governance Systems.....	1477
1. The European Union's <i>Ex Ante</i> Model: Preventive, Rights-Oriented Regulation.....	1477
2. The United States' <i>Ex Post</i> Model: Reactive, Fragmented, and Litigation-Driven	1482
3. The Industry-Led or Self-Regulatory Model: Adaptive and Business-Responsive.....	1486
i. Self-Regulatory Organizations Defined	1486
ii. The Ideal Biometric AI Hypothetical Model.....	1489
II.COMPARATIVE ANALYSIS OF REGIMES	1492
A. Grading the European Union and the United States	1492
1. Individual Rights Protection.....	1494

i. The European Union.....	1494
ii. The United States.....	1497
2. Incentives for Innovation.....	1501
i. The European Union.....	1501
ii. The United States.....	1506
3. Enforcement, Regulatory Effectiveness & Accountability	1508
i. The European Union.....	1508
ii. The United States.....	1515
B. Applied Case Studies: Comparative Illustrations.....	1518
1. Identity Authentication and User Verification: United States Response to Meta.....	1519
2. Deepfake Detection and Content Authentication: EU Response to Meta	1521
3. Iterative AI Training and Consent: The BIPA Response to Amazon.....	1522
i. Illinois BIPA Class Action: Amazon Photos and Rekognition	1523
ii. COVID-19 Workplace Data and AWS Liability.....	1524
iii. Broader Regulatory and Market Implications.....	1526
4. Law Enforcement and Mass Identification: United States and EU Response to Clearview AI.....	1527
i. United States Enforcement and Settlement Dynamics	1528
ii. The EU's GDPR Response to Clearview	1531
iii. Comparative Implications	1533
III.THE SELF-REGULATORY SOLUTION.....	1534
A. The European Union SRO	1535
B. The United States SRO.....	1538
C. The Pros and Cons of the Self-Regulatory Model	1541
IV.CONCLUSION.....	1544

I. UNDERSTANDING THE WORLD OF BIOMETRIC AI GOVERNANCE

A. Defining Biometric Data and Its Relationship with Artificial Intelligence

Biometric data is information derived from measurable human characteristics that can be used to recognize, authenticate, or identify an individual.¹ It captures physical traits, such as fingerprints, facial features, iris patterns, and hand geometry; as well as behavioral traits, including voice, gait, typing patterns, and other interaction signatures.² In operational systems, these traits are typically converted into biometric templates, known as feature vectors, that encode distinguishing characteristics in a format suitable for storage, comparison, and matching.³ Biometric systems are generally deployed for either authentication (one-to-one verification, asking whether a person is who they claim to be) or identification (one-to-many matching, asking who a person is within a larger population).⁴

Unlike most forms of personal data, biometric identifiers are intrinsically linked to an individual's body and behavior, making them effectively non-fungible and largely impossible to replace or revoke once compromised.⁵ Because biometrics function as a direct bridge between physical identity and digital access, their non-transferable nature enhances security while simultaneously amplifying privacy and civil liberties risks, particularly when such systems are deployed at scale or without meaningful safeguards.⁶

1. See *What Is the Difference Between Physiological and Behavioral Biometrics?*, AWARE (Dec. 8, 2022), <https://www.aware.com/blog-difference-between-physiological-and-behavioral-biometrics/> [https://perma.cc/SSV6-WWAE] [hereinafter *Physiological and Behavioral Biometrics*].

2. See *id.*

3. See *Biometric Data*, INNOVATRICS, <https://www.innovatrics.com/glossary/biometric-data/> [https://perma.cc/ZZ36-LLNP] (last visited Dec. 24, 2025).

4. See *What Is Biometrics?*, IDEMIA, <https://www.idemia.com/biometrics> [https://perma.cc/S6JX-78Q3] (last visited Dec. 24, 2025).

5. See *Physiological and Behavioral Biometrics*, *supra* note 1.

6. See *The Complex Relationship Between Biometrics and Artificial Intelligence*, BIOMETRICS INST. (Jan. 23, 2025), <https://www.biometricsinstitute.org/the-complex-relationship-between-biometrics-and-artificial-intelligence/> [https://perma.cc/PA96-A55K] [hereinafter *Complex Relationship*].

Today, biometric technologies have become a routine feature of everyday life, embedded across a wide range of sectors, including security, commerce, law enforcement, and public administration.⁷ The most familiar applications involve consumer authentication, such as fingerprint scans or facial recognition used to unlock smartphones, access financial accounts, or authenticate users on digital platforms.⁸ Technologies that once seemed revolutionary and futuristic are now seamlessly integrated into consumer-facing services, from voice-controlled virtual assistants to identity-enabled services in retail and entertainment settings.⁹ Beyond consumer devices, biometrics are increasingly deployed in high-friction identity environments, such as airports and border crossings, where automated biometric gates and identity verification systems are utilized to enhance security while streamlining passenger flow.¹⁰ Financial institutions similarly rely on biometric verification during customer onboarding and online transactions to mitigate instances of fraud and identity theft.¹¹ In the private sector, biometric systems support access control, workforce management, and commercial analytics.¹² Law enforcement agencies also utilize biometric matching to identify suspects or locate missing persons.¹³ Ultimately, these expanding applications give rise to well-documented risks, including identity theft following data breaches, mass or remote surveillance by governments, and discriminatory profiling when biometric categorization is tied to sensitive attributes or automated decision-making systems.¹⁴

7. See *What Is Biometrics?*, *supra* note 4.

8. See *id.*

9. See, e.g., *Amazon One Palm Payment Technology Is Coming to All 500+ Whole Foods Market Stores in the U.S.*, AMAZON NEWSROOM (July 20, 2023), <https://www.aboutamazon.com/news/retail/amazon-one-whole-foods-market-palm-scanning> [<https://perma.cc/J4CV-MKW3>] (demonstrating the increasing use of biometric technologies in a consumer-focused industry).

10. See *What Is Biometrics?*, *supra* note 4.

11. See *The Rise of Digital Banking*, AWARE (May 4, 2023), <https://www.aware.com/blog-the-rise-of-digital-banking/> [<https://perma.cc/9W85-Q8P6>].

12. See, e.g., *Workforce Management Solutions*, BIOMETRIC UPDATE, <https://www.biometricupdate.com/service-directory/workforce-management> [<https://perma.cc/NY8R-VX5G>] (last visited Aug. 23, 2026).

13. See *What Is Biometrics?*, *supra* note 4.

14. See Lauren Hendrickson, *Privacy Concerns With Biometric Data Collection*, IDENTITY (Dec. 11, 2025), <https://www.identity.org/privacy-concerns-with-biometric-data-collection/> [<https://perma.cc/J67M-LYMP>].

As biometric technologies have expanded alongside advances in artificial intelligence (AI), their relationship with AI has become a focal point of both technical development and regulatory contestation.¹⁵ In this context, AI refers to computational systems capable of learning from biometric data, recognizing patterns, and making adaptive decisions.¹⁶ When applied in this way, AI significantly enhances analytic speed, accuracy, and scalability, transforming biometrics from localized verification tools into infrastructures capable of monitoring and understanding an entire population.¹⁷

Biometrics Institute, a global organization focused on ethical standards and governance in biometric technology, published a paper in 2024, which documents “unprecedented disagreement” within the biometrics community over whether biometric systems are inherently intertwined with AI or whether they can exist independently.¹⁸ This disagreement highlights a fundamental fault line in contemporary biometric governance: whether biometric regulation can remain technologically neutral, or whether the increasing reliance on machine learning fundamentally alters the risk profile, scale, and social implications of biometric systems.¹⁹ The Institute observes that public and media discourse frequently collapses distinctions between biometric modalities, system functions, and algorithmic techniques, creating persistent “technical ambiguity.”²⁰ For governance purposes, this ambiguity matters because regulatory debates often conflate AI with facial recognition or treat biometric surveillance as synonymous with AI itself, resulting in rules, if they exist at all, that are poorly calibrated to specific technologies and use cases.²¹

The complexity of this relationship is most visible with the rise of behavioral biometrics, which shifts biometric identification

15. See *Complex Relationship*, *supra* note 6.

16. See Adib Bin Rashid & MD Ashfakul Karim Kausik, *AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications*, 7 HYBRID ADVANCES 100277, 100277 (2024).

17. See *id.*

18. See *Complex Relationship*, *supra* note 6.

19. See *Members' Viewpoints: The Relationship Between Biometrics and Artificial Intelligence (AI)*, BIOMETRICS INST. (Jan. 23, 2025), <https://www.biometricsinstitute.org/members-viewpoints-the-relationship-between-biometrics-and-artificial-intelligence-ai/> [<https://perma.cc/CB69-FBRB>].

20. See *Complex Relationship*, *supra* note 6.

21. See *id.*

away from static traits and toward continuous, model-driven pattern recognition.²² As discussed earlier, behavioral biometrics evaluate how users interact with devices in real time, by their typing cadence, swipe gestures, navigation behavior, or device handling.²³ In this context, identity verification becomes an ongoing process, rather than a discrete authentication event: the biometric identifier is no longer merely an underlying data stream, but the AI-driven inference that translates behavioral signals into an evolving identity profile.²⁴ AI becomes the enabling condition that makes behavioral biometrics viable at scale.²⁵ Machine learning models construct adaptive behavioral profiles that evolve as users change over time, and support real-time anomaly detection through unsupervised learning techniques, allowing systems to detect suspicious deviations without requiring perfectly labeled fraud data.²⁶ In essence, the biometric value of behavioral signals depends on the AI's capacity to extract patterns, predict anomalies, and continuously recalibrate normal behavior for a given individual.²⁷ This dynamic explains why some experts view biometrics and AI as inherently intertwined: many modern biometric systems no longer function as simple matching systems, but as adaptive inference engines that assess both identity and risk simultaneously.²⁸ The more behavioral, continuous, and context-dependent a biometric system becomes, the more it tends to rely on AI to make its outputs meaningful and scalable.²⁹

AI integration of this sort ultimately reshapes the normative stakes of biometric deployment. Continuous monitoring can enable sensitive inferences, such as stress levels, cognitive impairment, or disability-related patterns, that extend beyond the original purpose of identity verification.³⁰ When biometric systems generate these secondary inferences, they undermine purpose

22. See Zennon Kapron, *Beyond the Swipe: How Artificial Intelligence Is Redefining Biometrics*, FORBES (Jan. 27, 2025), <https://www.forbes.com/sites/zennonkapron/2025/01/27/beyond-the-swipe-how-artificial-intelligence-is-redefining-biometrics/> [https://perma.cc/53NQ-PGEM].

23. See *Physiological and Behavioral Biometrics*, *supra* note 1.

24. See *id.*

25. See Kapron, *supra* note 22.

26. See *id.*

27. See *id.*

28. See *id.*

29. See *id.*

30. See *id.*

limitations by transforming identification data into behavioral or health proxies, increasing the likelihood of repurposing without meaningful consent.³¹

Taken together, these dynamics demonstrate why biometric data is increasingly situated at the intersection of privacy law and AI governance. Biometric identification supplies the identity objective, AI provides the adaptive inferential capacity, and governance frameworks determine whether these systems are deployed in ways that are lawful, ethical, and socially legitimate.³² As biometric systems become more automated, scalable, and behaviorally granular, the relationship between biometrics and AI is best understood as conditional, but increasingly convergent—amplifying both the technological capability and the need for robust governance.³³

Because biometric data is profoundly personal, misuse or abuse can have severe consequences, reinforcing the need for governance frameworks capable of managing the risks associated with such a level of complexity.³⁴ AI biometric governance therefore functions as the framework through which societies seek to manage these risks while preserving legitimate and beneficial uses.³⁵ Establishing standards and oversight for data protection, accuracy, fairness, accountability, and lawful deployment ensures that biometric systems are both technically effective and normatively justified.³⁶ In simple terms, governance efforts focus on establishing rules about how biometric data is collected and stored, how AI models are trained and evaluated, and how responsibility is allocated when systems produce harmful or erroneous outcomes.³⁷

With this effort comes governance challenges that extend beyond technical considerations into structural aspects.³⁸ AI-driven biometrics operate at the intersection of identity,

31. *See id.*

32. *See AI Biometric Governance*, PRISM SUSTAINABILITY DIRECTORY (May 10, 2025), <https://prism.sustainability-directory.com/term/ai-biometric-governance/> [<https://perma.cc/NPN4-UWWU>].

33. *See id.*

34. *See id.*

35. *See id.*

36. *See id.*

37. *See id.*

38. *See id.*

automation, and power, meaning that oversight failures can have systemic consequences far greater than isolated harms.³⁹ Effective governance frameworks should thus be designed to prevent dystopian outcomes, like pervasive public surveillance without consent or accountability, by embedding ethical constraints and legal safeguards directly into the lifecycle of biometric AI systems.⁴⁰

Seen this way, biometric data provides the raw identity substrate, AI supplies the analytical and inferential capacity, and governance supplies the normative boundary conditions that determine whether such systems serve legitimate social objectives or undermine fundamental rights.⁴¹ This triadic relationship explains why biometric regulation is increasingly overlapping with AI governance and why contemporary policy debates treat biometric systems not simply as data-processing tools, but as AI-enabled infrastructures that require heightened regulatory attention.⁴²

B. Description of the Three Governance Systems

1. The European Union's *Ex Ante* Model: Preventive, Rights-Oriented Regulation

The European Union's *ex ante* regulatory model for biometrics and AI is grounded in the principle that technologies posing systemic risks to fundamental rights must be governed before deployment.⁴³ This approach reflects the EU's commitment to human dignity, privacy, data protection, and proportionality as referenced in the Charter of Fundamental Rights of the European Union (hereinafter, the "EU Charter").⁴⁴ Similar rights-based principles have increasingly shaped European efforts to regulate

39. See *id.*

40. See *id.*

41. *Id.*

42. *Id.*

43. See *EU AI Act: First Regulation on Artificial Intelligence*, EUR. PARL. (Feb. 19, 2025), <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> [<https://perma.cc/UG2E-LVNK>].

44. See Charter of Fundamental Rights of the European Union, arts. 1, 7–8, 52, 2012 O.J. (C 326) 391.

emerging technologies.⁴⁵ In the biometric-AI context, the EU treats biometric systems as inherently rights-sensitive infrastructures capable of enabling mass surveillance, discrimination, and irreversible harm.⁴⁶

The EU's General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) collectively form the core of the EU's *ex ante* governance framework for biometric AI systems.⁴⁷ Their combined architecture is oriented around prevention before harm occurs and embedding rights protections within system design, rather than relying solely on after-the-fact remediation.⁴⁸

The GDPR defines "biometric data" as personal data resulting from specific technical processing of an individual's physical, physiological or behavioral characteristics, that enables or confirms unique identification, such as facial images or fingerprint data.⁴⁹ When biometric data is used for the purpose of uniquely identifying a natural person, the GDPR would classify this as a "special category of personal data" a form of processing that is generally prohibited under Article 9(1).⁵⁰ Article 9(2) provides an exhaustive list of exceptions to this prohibition, permitting processing only when one of the enumerated legal grounds applies, such as explicit consent or substantial public interest subject to safeguards.⁵¹ As a result, biometric-AI systems deployed within the

45. See EUR. COMM'N FOR THE EFFICIENCY OF JUST. (CEPEJ), EUROPEAN ETHICAL CHARTER ON THE USE OF ARTIFICIAL INTELLIGENCE IN JUDICIAL SYSTEMS AND THEIR ENVIRONMENT 15 (2018), <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> [https://perma.cc/P97S-NVSN].

46. See GLORIA GONZÁLEZ FUSTER & MICHALINA NADOLNA PEETERS, PERSON IDENTIFICATION, HUMAN RIGHTS AND ETHICAL PRINCIPLES: RETHINKING BIOMETRICS IN THE ERA OF ARTIFICIAL INTELLIGENCE 2–3 (Eur. Parl. Rsch. Serv., PE 697.191, 2021), [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU\(2021\)697191_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf) [https://perma.cc/9MAK-J85S].

47. See Richard Lawne, *Biometrics in the EU: Navigating the GDPR and AI Act*, INT'L ASS'N OF PRIV. PROS. (Apr. 23, 2025), <https://iapp.org/news/a/biometrics-in-the-eu-navigating-the-gdpr-ai-act/> [https://perma.cc/VN54-ZU4Q].

48. Alessandro Mantelero & Maria Samantha Esposito, *An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems*, 41 COMPUT. L. & SEC. REV. 105561, 105568 (2021).

49. 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), art. 4, 2016 O.J. (L 119) 1 [hereinafter GDPR].

50. *Id.*

51. *Id.*; see also *What Are the Conditions for Processing?*, INFO. COMM'R'S OFF., <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special->

EU must either avoid processing biometric data for unique identification altogether or satisfy a two-step test by establishing both a lawful basis under Article 6,⁵² and a specific exception under Article 9.⁵³ Scholars emphasize that this regulatory design places the individual's rights and fundamental freedoms at the very center of governance and makes their protection a precondition for biometric-system deployment.⁵⁴

The EU AI Act ("the Act") complements the data protection regime by introducing a comprehensive, risk-based classification of AI systems.⁵⁵ The Act evaluates biometric systems based on their potential impact on health, safety, and fundamental rights, explicitly recognizing that biometric uses vary significantly in risk depending on the context and application.⁵⁶ For example, the Act defines a "remote biometric identification system" as an AI system intended to identify natural persons without their active involvement, typically at a distance, by comparing biometric data with a reference database.⁵⁷ It further distinguishes between a "real-time biometric identification system," where capture, comparison, and identification occur without significant delay, and a "post-remote biometric identification system," which does not

category-data/what-are-the-conditions-for-processing/ [https://perma.cc/HM6B-2RZ4] (last visited Mar. 14, 2026).

52. Article 6 of the GDPR, "Lawfulness of Processing" enumerates six possibilities of a legal processing: [a] the data subject has given consent to the processing of his or her personal data for one or more specific purposes; [b] processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; [c] processing is necessary for compliance with a legal obligation to which the controller is subject; [d] processing is necessary in order to protect the vital interests of the data subject or of another natural person; [e] processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; [f] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. *See* GDPR, *supra* note 49, art. 6.

53. GDPR, *supra* note 49, art. 9, at 38.

54. *See* T. Bisztray et al., *Emerging Biometric Modalities and Their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks*, in *PROC. 2021 INT'L CONF. OF THE BIOMETRICS SPECIAL INT. GRP. (BIOSIG)* 1, 1–5 (2021), <https://ieeexplore.ieee.org/document/9548298> [https://perma.cc/8AUW-7KGJ].

55. *See* Leire Arbona, *Updated Overview: The European Union's Artificial Intelligence Act*, VERIDAS (Feb. 20, 2025), <https://veridas.com/en/artificial-intelligence-act/> [https://perma.cc/7WKV-NAF8].

56. *Id.*

57. *See* Lawne, *supra* note 47.

fulfill the same “real-time” criteria.⁵⁸ The Act establishes a general prohibition on the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement, subject only to narrowly tailored exceptions.⁵⁹ Article 5(1)(h) permits such use solely where it is strictly necessary for (i) the targeted search of victims of specific crimes, such as human trafficking; (ii) the prevention of a threat to life or physical safety of persons, or of a terrorist attack; or (iii) the localization or identification of a person suspected of having committed a criminal offense where necessary for investigation, prosecution, or execution of a penalty, provided that the offense is listed in Annex I and punishable under national law by a maximum sentence of at least four years.⁶⁰ Critics have argued that while the first two purposes appear relatively straightforward and coherent, the third exception introduces potential fragmentation, especially because there has not yet been a widely reported, fully implemented case that can offer interpretive guidance.⁶¹ Annex II of the Act contains an exhaustive list of sixteen criminal offenses, but these offenses lack a common European definition, raising concerns about divergent national interpretations and uneven application across the EU’s Member States.⁶² Beyond identification systems, the Act also classifies biometric categorization systems, those that assign individuals to categories based on biometric data, including inferred attributes like age, gender, ethnicity, and emotional state, as “high risk.”⁶³ This designation triggers extensive compliance obligations,

58. See *id.*; see also Jaden Deibo, *The Balancing Act: How the European Union’s Artificial Intelligence Act Properly Frames the Dangers and Benefits of Using Biometric Identification to Combat Human Trafficking*, MICH. J. INT’L L. ONLINE (Oct. 2024), <https://www.mjilonline.org/the-balancing-act-how-the-european-unions-artificial-intelligence-act-properly-frames-the-dangers-and-benefits-of-using-biometric-identification-to-combat-human-trafficking/> [https://perma.cc/8VVM-LSYH].

59. Regulation (EU) 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), art. 5, 2024 O.J. (L 1689) 1 [hereinafter AI Act].

60. See Alice Gianni & Sarah Tas, *AI Act and the Prohibition of Real-Time Biometric Identification*, VERFASSUNGSBLOG (Dec. 10, 2024), <https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/> [https://perma.cc/G6N4-SW5V].

61. See *id.*

62. *Id.*

63. AI Act, *supra* note 59.

including requirements around data governance, human oversight, and registration in the EU's database.⁶⁴

Together, the GDPR and the EU AI Act create an interlocking, layered governance regime that regulates both the processing of personal data through AI systems and the development and use of the systems themselves. The GDPR governs whether and how personal data may be processed, requiring controllers to establish a lawful basis for processing. Where applicable, heightened protections for special-category data must be satisfied and their corresponding high-risk processing must be assessed through a data protection impact test before that processing occurs. The EU AI Act operates alongside these requirements by regulating AI systems according to their uses and risk classifications, imposing distinct obligations on providers and deployers, including prohibited-use rules, conformity requirements, and operational safeguards. Thus, an organization deploying a biometric-AI system may be subject simultaneously to the GDPR's requirements governing the underlying processing of data as well as the AI Act's requirements governing the development or use of the AI system itself.

This dual framework reflects the EU's commitment to "privacy by design" and "data protection through technology design."⁶⁵ It embeds human rights considerations and precautionary governance directly into the architecture of biometric-AI system deployment, rather than treating rights protection as an external constraint.⁶⁶ Scholars accordingly characterize the EU approach as a preventative regulatory regime, in which compliance is a condition of deployment, rather than a response to demonstrated harm, in line with the 'Preparedness Union Strategy.'⁶⁷ This model exemplifies the EU's broader commitment to *ex ante* regulation and anticipatory governance,

64. See Lawne, *supra* note 47.

65. See *GDPR Privacy by Design*, INTERSOFT CONSULTING, <https://gdpr-info.eu/issues/privacy-by-design/> [<https://perma.cc/WEE6-KDHD>] (last visited Nov. 12, 2025).

66. See *id.*

67. See *Preparedness Union Strategy: Reinforcing Europe's Resilience in a Changing World*, EUR. UNION EXTERNAL ACTION (Mar. 3, 2025), https://www.eeas.europa.eu/eeas/preparedness-union-strategy_en [<https://perma.cc/8ZJJ-RJ3S>] [hereinafter *Preparedness Union Strategy*]; see also *Peace, Stability and Conflict Prevention*, EUR. COMM'N, https://fpi.ec.europa.eu/what-we-do/peace-stability-and-conflict-prevention_en [<https://perma.cc/G6E9-258X>] (last visited Nov. 12, 2025).

embedding human rights and precautionary principles into biometric-AI systems before they are allowed to operate within society.⁶⁸

2. The United States' *Ex Post* Model: Reactive, Fragmented, and Litigation-Driven

The United States regulates biometric data primarily through state-level statutes, private litigation, and federal enforcement under general consumer protection laws rather than through a comprehensive federal biometric-AI regime.⁶⁹ These statutes tend to guide regulation only after the fact, in an *ex post* fashion, rather than imposing binding pre-deployment constraints.⁷⁰

Protecting biometric data is one of many issues facing regulators in the United States, primarily at the state and local levels, where significant privacy legislation has emerged in the absence of comprehensive federal privacy law.⁷¹ Although twelve states have adopted general data privacy statutes, only three states and one city (Illinois, Texas, Washington, and New York City) currently have privacy laws specific to biometric data in place.⁷² Among the three states, Illinois' statute is regarded as the most potent and impactful due to its breadth and unique private right of action.⁷³

The Illinois Biometric Information Privacy Act (BIPA) was enacted in 2008 and grants Illinois residents enforceable rights over their biometric data.⁷⁴ The statute defines "biometric information" broadly to include any information, regardless of how it is captured, converted, stored, or shared, derived from an individual's biometric identifier and used to identify that

68. See *Preparedness Union Strategy*, supra note 67.

69. See *Data Privacy and Biometric Technology Use*, THOMSON REUTERS (July 22, 2024), <https://www.thomsonreuters.com/en-us/posts/corporates/biometric-tech-use/> [<https://perma.cc/5PHT-VGXQ>].

70. See *id.*

71. See Lori S. Ross, *Biometric Data Protection: A Growing Trend in State Privacy Legislation*, OUTSIDE GC (Feb. 7, 2024), <https://www.outsidegc.com/blog/biometric-data-protection-a-growing-trend-in-state-privacy-legislation> [<https://perma.cc/PH8S-WT67>].

72. See *id.*

73. See *id.*

74. See *Illinois Biometric Information Privacy Act (BIPA)*, DYKEMA GOSSETT PLLC, <https://www.dykema.com/services/practices/privacy-and-data-security/illinois-biometric-information-privacy-act-bipa.html> [<https://perma.cc/W4AE-J4AG>] (last visited Mar. 12, 2026).

individual.⁷⁵ Section 15(b) prohibits private entities from collecting or otherwise obtaining biometric identifiers or information unless they first provide written notice specifying the data collected, the purpose of collection, and the duration of retention, and obtain the individual's written informed consent.⁷⁶ To add to these notice-and-consent requirements, the statute categorically prohibits the sale, lease, trade, or other monetization of biometric data.⁷⁷

Notably, BIPA is the first biometric privacy statute in the United States to include a private right of action.⁷⁸ Any individual “aggrieved” by a violation of BIPA may bring a suit and recover statutory or actual damages, reasonable attorneys’ fees and costs, and injunctive relief.⁷⁹ The statute authorizes liquidated damages of \$1,000 per negligent violation and \$5,000 per intentional or reckless violation, making procedural noncompliance itself a source of potentially significant liability even when a plaintiff does not establish actual damages.⁸⁰

Since its enactment, BIPA has generated extensive litigation, which has surged following key judicial decisions holding that plaintiffs could pursue claims for certain statutory violations without demonstrating additional actual harm resulting from those violations, thereby expanding the incentive to litigate alleged noncompliance.⁸¹ The most consequential decision was the Illinois Supreme Court’s ruling in *Rosenbach v. Six Flags Entertainment Corp.* in 2019, which held that a plaintiff need not allege an additional injury or adverse consequence beyond the violation of BIPA’s statutory requirement to qualify as a “person aggrieved”

75. See Chris Wager, *Biometric Privacy Laws: What Businesses Need to Know Right Now*, MACMURRAY & SHUSTER LLP (Aug. 5, 2024), <https://mslawgroup.com/biometric-privacy-laws-what-businesses-need-to-know-right-now/> [https://perma.cc/4U22-742G].

76. See *id.*

77. Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15 (2024) [hereinafter BIPA].

78. See Blake Fensom et al., *The Who, Why, and Where of Biometric Privacy Litigation: An Empirical Analysis of BIPA Cases 2015–2024*, ANTITRUST SOURCE, June 2025, at 3, <https://www.americanbar.org/content/dam/aba/publications/antitrust/source/2025/june/biometric-privacy-litigation.pdf> [https://perma.cc/6BYT-CPJY].

79. See *id.*

80. BIPA § 20.

81. See Fensom et al., *supra* note 78, at 3.

under the Act.⁸² Further momentum followed the first jury verdict in a BIPA case, *Rogers v. BNSF Railway Company*, in 2022.⁸³

The significant size of BIPA class action settlements in recent years also underscores the extent of potential liability that private entities may face.⁸⁴ Examples include TikTok's \$92 million settlement in 2022 over allegations that it collected users' facial geometry without consent; Bumble and Badoo's \$40 million settlement over allegations that they unlawfully collected facial-geometry scans from photographs uploaded to their dating applications; Kronos Inc.'s \$15.3 million settlement in 2022 with employees who scanned their fingerprints using Kronos-branded time clocks; and BNSF's \$75 million settlement in 2024 concerning its use of fingerprint scans from drivers entering company facilities through automated gate systems.⁸⁵ These high-profile settlements under BIPA demonstrate how lawsuits substitute for administrative regulation, incentivizing firms to review biometric-data practices even in the absence of national regulation.⁸⁶ A significant share of BIPA litigation has centered on Section 15(b), and particularly, disputes over whether violations occur only at the initial collection of biometric data or recur with each subsequent scan performed without valid consent.⁸⁷

82. See *id.*; see, e.g., *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶¶ 1–2.

83. See Fensom et al., *supra* note 78, at 9; see, e.g., *Rogers v. BNSF Ry. Co.*, 63 F.4th 1068 (7th Cir. 2023).

84. See Fensom et al., *supra* note 78, at 11.

85. See *id.*; see also *In re TikTok, Inc. Consumer Priv. Litig.*, 565 F. Supp. 3d 1076, 1081–82 (N.D. Ill. 2021); *Howell v. Bumble Trading LLC*, No. 2021-L-307 (Ill. Cir. Ct. Oct. 24, 2024); *Figueroa v. Kronos Inc.*, No. 19-cv-1306 (N.D. Ill. Feb. 18, 2022); *Rogers v. BNSF Ry. Co.*, 680 F. Supp. 3d 1027 (N.D. Ill. 2023).

86. See Fensom et al., *supra* note 78, at 11.

87. See Brett M. Doran, Tiffany S. Fordyce, Jena M. Valdetero & Zachary Pestine, *BIPA Update: Illinois Limits Liability and Clarifies Electronic Consent for Biometric Data Collection*, GREENBERG TRAURIG (Aug. 14, 2024), <https://www.gtlaw.com/en/insights/2024/8/bipa-update-illinois-limits-liability-and-clarifies-electronic-consent-for-biometric-data-collection> [https://perma.cc/2JRX-FUE2]. Courts have long debated whether BIPA liability attaches only to the initial collection of biometric data or to each subsequent scan conducted without proper consent. The issue had enormous implications for damages. For example, an employee scanning a fingerprint twice daily could generate more than 500 scans annually; if each scan constituted a separate violation subject to up to \$5,000 in statutory damages, potential liability could exceed \$2.5 million per employee per year. For an employer with 1,000 employees, damages could theoretically reach \$2.5 billion annually. In *Cothron v. White Castle Systems, Inc.* (2023), the Illinois Supreme Court held that each scan or transmission without proper consent constitutes a separate violation under Sections 15(b) and 15(d), significantly expanding potential liability even

Similarly, Texas enacted the Capture or Use of Biometric Identifier Act (CUBI), and Washington enacted HB 1493, both of which regulate biometric data, but differ significantly in scope, enforcement mechanisms, and remedies.⁸⁸ Other states regulate biometric data indirectly through general privacy statutes, and numerous cities, including New York City and Portland, have enacted laws that regulate law enforcement's use of facial recognition technology.⁸⁹ The result is a patchwork regulatory landscape, with inconsistent definitions, rights of action, and compliance obligations across jurisdictions.

At the federal level, no statute directly governs the collection, use, storage, or disclosure of biometric data.⁹⁰ However, Section 5 of the Federal Trade Commission Act (FTCA) authorizes the Federal Trade Commission (FTC) to prohibit unfair and deceptive trade practices in or affecting commerce.⁹¹ In a policy statement issued May 18, 2023, the FTC reaffirmed its commitment to combating biometric data abuse, and identified a non-exhaustive set of practices that may violate Section 5, including inadequate safeguards, deceptive consent practices, and misuse of biometric technologies.⁹²

Compliance with biometric governance has thus emerged primarily through deterrence via litigation risk, rather than through mandatory design obligations or pre-market approval. At the same time, this model invites fragmentation and uncertainty.⁹³ Divergent state laws create asymmetric risk exposure and compliance complexity, while ambiguous statutory language

where no concrete injury is shown. *See Cothron v. White Castle Sys., Inc.*, 2023 IL 128004. Shortly after the decision, the Illinois General Assembly enacted SB2979, limiting recovery to a single violation per individual for repeated collections or disclosures of biometric data, thereby placing guardrails on the potentially catastrophic damages suggested by *Cothron*.

88. *See Data Privacy and Biometric Technology Use*, *supra* note 69.

89. *See id.*

90. *See id.*

91. *See id.*

92. *See Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, FED. TRADE COMM'N (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf [<https://perma.cc/ZJ62-W525>] [hereinafter FTC Biometric Policy Statement].

93. *See William Walter Finch & Marya Butt, Gaps in AI-Compliant Complementary Governance Frameworks' Suitability (for Low-Capacity Actors), and Structural Asymmetries (in the Compliance Ecosystem)—A Systematic Review*, 5 J. CYBERSECURITY & PRIV. 101 (2025).

leaves firms uncertain about how liability attaches.⁹⁴ Scholars identify persistent “tensions between legal and technical considerations” under BIPA that may affect innovation and deployment.⁹⁵ Critics also argue that the threat of high liability may chill the use of biometric AI systems or push firms to avoid certain deployments.⁹⁶

3. The Industry-Led or Self-Regulatory Model: Adaptive and Business-Responsive

i. Self-Regulatory Organizations Defined

A self-regulatory organization (SRO) is a private, membership-based institution through which industry participants collectively develop, implement, and enforce standards governing member conduct, typically under some degree of public oversight.⁹⁷ In the context of biometric-AI governance, no such SRO currently exists. Nevertheless, a network of industry-led, jurisdictionally specific SROs would represent a viable regulatory model grounded in well-established precedents across financial markets, advertising, and cybersecurity,⁹⁸ and would occupy the conceptual space between the European Union’s *ex ante*, state-centered regime and the United States’ *ex post*, litigation-driven approach.

Rather than relying primarily on direct legislative command or retrospective liability, this model would emphasize private coordination, collective standard-setting, and peer-based enforcement.⁹⁹ Governance would operate primarily through soft

94. *See id.*; *see generally* Eliza Simons, *Putting a Finger on Biometric Privacy Laws: How Congress Can Stitch Together the Patchwork of Biometric Privacy Laws in the United States*, 86 BROOK. L. REV. 1097, 1107–10 (2021).

95. *See* Rui-Jie Yew & Alice Xiang, *Regulating Facial Processing Technologies: Tensions Between Legal and Technical Considerations in the Application of Illinois BIPA*, in PROC. 2022 ACM CONF. ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY (FACCT ’22) 1017, 1017–29 (2022), <https://doi.org/10.1145/3531146.3533163> [<https://perma.cc/72SE-7AAS>].

96. *See* Brief of Internet Ass’n as Amicus Curiae in Support of Defendant-Appellee at 17–18, *Cothron v. White Castle Sys., Inc.*, 20 F.4th 1156 (7th Cir. 2021) (No. 20-3202) (arguing that expansive BIPA liability would “chill innovation”).

97. *See* Adam Hayes, *Self-Regulatory Organization (SRO): Definition and Examples*, INVESTOPEDIA (Feb. 11, 2025), <https://www.investopedia.com/terms/s/sro.asp> [<https://perma.cc/D7W3-FV88>].

98. *See id.*

99. *See id.*

law mechanisms, including internal compliance processes, third-party audits, transparency commitments, and certification requirements that can evolve more rapidly than statutory regulations.¹⁰⁰ In practice, such a framework would function as co-regulation, combining industry expertise with residual public oversight similar to consumer protection authorities in the United States or recognized conformity assessment bodies in the EU. The objective is to establish predictable and interoperable compliance standards that safeguard consumers while maintaining flexibility for rapidly evolving biometric technologies, enabling the industry to address challenges and stakeholder concerns in real-time.¹⁰¹

Analogous institutions in other regulated sectors demonstrate that private governance operating under public supervision can promote both innovation and consumer protection.¹⁰² This model would therefore complement, rather than substitute, public law regimes. As former Commodity Futures Trading Commission (CFTC) Chairman Heath Tarbert observed in the context of derivatives, sound regulation “does not require choosing between governmental and private action.”¹⁰³ Instead, the most stable regulation “blend[s] the expertise and adaptability of private-sector influence with the stabilizing effects of federal oversight.”¹⁰⁴ The derivatives markets provide a canonical example.¹⁰⁵ Their century-long history of self-regulation, culminating in exchanges like the Chicago Board of Trade (CBOT) and later overseen by the CFTC, demonstrates how markets can effectively police themselves when a public regulator supervises the framework.¹⁰⁶

Financial market SROs, including national securities exchanges and securities associations such as the New York Stock

100. See Eric D. Reicin, *The Case for Teaching Industry Self-Regulation in Law, Business, and Public Policy Schools*, BBB NAT'L PROGRAMS (Dec. 9, 2024), <https://bbbprograms.org/media/insights/blog/teaching-industry-self-regulation> [<https://perma.cc/BB9P-P2TQ>].

101. See *id.*

102. See Kevin T. Frazier, *The Case for Private AI Governance*, REGUL. REV. (Aug. 26, 2025), <https://www.theregreview.org/2025/08/26/frazier-the-case-for-private-ai-governance/> [<https://perma.cc/3Z5K-UDAY>].

103. See Heath P. Tarbert, *Self-Regulation in the Derivatives Markets: Stability Through Collaboration*, 41 NW. J. INT'L L. & BUS. 175, 178 (2021).

104. See *id.*

105. See *id.* at 179.

106. See *id.*

Exchange (NYSE), NASDAQ, and the Financial Industry Regulatory Authority (FINRA), further illustrate how private institutions can draft and enforce industry rules under public authorization while maintaining accountability.¹⁰⁷ Under Sections 6 and 15A of the Securities Exchange Act of 1934, the Securities and Exchange Commission (SEC) authorizes national exchanges and securities associations to establish and enforce their own rules governing member conduct, investigate violations, and maintain investor trust, subject to SEC oversight and approval.¹⁰⁸ This hybrid structure, composed of private rulemaking and public supervision, demonstrates how technical specialization, peer enforcement, and public accountability can coexist, offering a governance template that could be adapted for biometric AI oversight.¹⁰⁹

Comparable dynamics appear in other sectors. In digital advertising, industry organizations have developed privacy codes requiring notice, opt-out mechanisms, and data handling transparency, enforced through membership conditions and reputational sanctions.¹¹⁰ In cybersecurity and data protection, voluntary standards such as the NIST Cybersecurity Framework and internationally recognized ISO/IEC 27001 have functioned as *de facto* regulatory instruments, frequently referenced by agencies and courts as indicators of reasonable care.¹¹¹

107. See Hayes, *supra* note 97.

108. Securities Exchange Act of 1934, 15 U.S.C. §§ 78a–78qq (2024).

109. See Frazier, *supra* note 102.

110. See NAI Announces Framework for New Era of Digital Advertising Self-Regulation, NETWORK ADVERT. INITIATIVE (Mar. 10, 2025), <https://thenai.org/press/nai-announces-framework-for-new-era-of-digital-advertising-self-regulation/> [https://perma.cc/L2L8-6Q88]; see also 2020 Code of Conduct, NETWORK ADVERT. INITIATIVE (2020), https://thenai.org/wp-content/uploads/2021/07/nai_code2020.pdf [https://perma.cc/SYW2-MW8U]; Lothar Determann & Andrew Folks, *Opting In-n-Out: Five Key Analyses for Adtech Privacy Law Compliance*, INT'L ASS'N OF PRIV. PROS. (Feb. 9, 2024), <https://iapp.org/news/a/opting-in-n-out-five-key-analyses-for-adtech-privacy-law-compliance/> [https://perma.cc/N547-K6GR].

111. See Katharina Koerner, *Standardization Landscape for Privacy: Part 1 - The NIST Privacy Framework*, INT'L ASS'N OF PRIV. PROS. (Dec. 1, 2021), <https://iapp.org/news/a/standardization-landscape-for-privacy-part-1-the-nist-privacy-framework/> [https://perma.cc/3VU4-LMCC]; see also Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N (Aug. 31, 2016), <https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-ftc> [https://perma.cc/RL4E-LDRS].

Beyond regulatory necessity, SRO membership offers strategic benefits to participating firms.¹¹² Membership signifies a firm's commitment to ethical conduct and regulatory compliance, thereby enhancing trust among consumers, partners, and investors. It would promote standardized practices that reduce ambiguity and compliance fragmentation, while rules developed by industry practitioners would better reflect operational realities than one-size-fits-all statutory mandates.¹¹³ Firms would also benefit from shared training resources, certification pathways, regulatory guidance, and dispute-resolution mechanisms, reducing both compliance costs and litigation exposure.¹¹⁴ Through collective monitoring and early risk identification, SROs would further help mitigate reputational and regulatory fallout.¹¹⁵

ii. The Ideal Biometric AI Hypothetical Model

The logic of self-regulation is well established in other technically complex and rapidly evolving sectors, especially financial services. Self-regulation typically involves a combination of private industry participation and government oversight, and has long been recognized as an effective and efficient regulatory approach in markets characterized by rapid innovation and high technical complexity.¹¹⁶ The central objectives of such systems include preserving market integrity through fair and transparent operations, maintaining financial stability by reducing systemic risk, and protecting participants from harmful or deceptive practices.¹¹⁷ In its most complete form, self-regulation grants an SRO the authority to create, amend, implement, and enforce rules of conduct governing entities within its jurisdiction, and the ability to resolve disputes through standardized mechanisms like arbitration.¹¹⁸ This authority is often derived from a statutory

112. See Team Atlan, *Self-Regulatory Organizations (SROs) Explained: How They Work and Why They Matter in 2025*, ATLAN (July 3, 2025), <https://atlan.com/know/data-governance/self-regulatory-organizations/> [<https://perma.cc/UG9S-HZN9>].

113. See *id.*

114. See *id.*

115. See Frazier, *supra* note 102.

116. INT'L ORG. OF SEC. COMM'NS, MODEL FOR EFFECTIVE REGULATION: REPORT OF THE SRO CONSULTATIVE COMMITTEE 1 (May 2000), <https://www.iosco.org/library/pubdocs/pdf/ioscopd110.pdf> [<https://perma.cc/TEC9-TKVS>].

117. See *id.*

118. See *id.* at 3.

delegation of power from a state to a non-governmental regulatory body.¹¹⁹ Historically, such institutions have emerged before formal statutory oversight as market participants recognized that those who were most familiar with customs, risks, and operational realities of a given industry were often best positioned to design and enforce effective rules.¹²⁰

An SRO is capable of establishing uniform technical and ethical standards governing data collection, consent verification, dataset curation, model training, deployment, and auditability.¹²¹ Membership can be conditioned on compliance with published codes of conduct and subject to periodic independent audits designed to verify adherence to these standards.¹²² To enhance transparency, SROs can maintain a public registry of compliant or certified entities, providing clear signals to consumers, investors, and regulators.¹²³ Credible enforcement would be essential to this model's legitimacy; therefore, a strong SRO could deploy a graduated system of sanctions, ranging from warnings and remedial directives to suspensions, public censure, or referral to statutory authorities in cases of persistent or egregious noncompliance.¹²⁴ Through these mechanisms, accountability would be embedded directly in market participation, rather than imposed solely through litigation or licensing.¹²⁵ Properly designed, such a framework can promote regulatory interoperability across jurisdictions, allowing firms to demonstrate compliance through a single, recognized certification.¹²⁶ This approach would reduce duplicative compliance costs while preserving adaptive, business-responsive oversight capable of evolving alongside biometric technologies.

Based on these reasons, and as demonstrated by well-established precedents like those of the financial market, SROs can be effective when compliance is tied to market participation, when reputational incentives reinforce adherence to standards, and when public institutions formally recognize these certification

119. *See id.*

120. *See id.* at 5.

121. *See Hayes, supra* note 97.

122. *See id.*

123. *See id.*

124. *See id.*

125. *See id.*

126. *See id.*

schemes or provide limited supervisory oversight.¹²⁷ More specifically, emerging technical and regulatory frameworks in each jurisdiction would provide the foundational infrastructure for a regionally grounded biometric-AI SRO. In the United States, the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (AI RMF) would serve as the most appropriate baseline for biometric governance.¹²⁸ The NIST AI RMF articulates a voluntary, risk-based approach to identifying, assessing, and mitigating AI risks via organizational processes structured through governance, mapping, measurement, and management.¹²⁹ Although not legally binding, it has become a widely referenced benchmark for reasonable care in AI development and deployment.¹³⁰ Its emphasis on shared risk terminology and procedural expectations aligns naturally with a US SRO model by supplying a common compliance language while leaving monitoring, certification, and enforcement to the SRO's institutional mechanisms. A biometric SRO would therefore incorporate the NIST AI RMF as its primary technical standard, supplementing it where appropriate, with jurisdiction-specific international norms, while providing the institutional enforcement, peer accountability, and public-facing legitimacy that technical standards alone cannot offer.¹³¹

In the EU, by contrast, a biometric-AI SRO could be established within the EU AI Act's risk-tiered regulatory framework. The Act already establishes substantive obligations, conformity assessment requirements, and oversight structures for high-risk AI systems, including biometric applications.¹³² An EU-based SRO would therefore operate as a complementary governance layer, translating statutory requirements into operational standards,

127. See, e.g., Team Atlan, *supra* note 112.

128. See *What Does NIST Mean for the World of Biometrics?*, ARATEK (Dec. 2, 2024), <https://www.aratek.co/news/what-does-nist-mean-for-the-world-of-biometrics> [<https://perma.cc/C24F-YAF3>].

129. *Id.*

130. See NAT'L INST. OF STANDARDS & TECH., ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (2023), <https://www.nist.gov/itl/ai-risk-management-framework> [<https://perma.cc/7KWT-TMG4>].

131. See ZenGRC Team, *Navigating the Future of AI Governance: A Guide to NIST AI RMF, ISO/IEC 42001, and the EU AI Act*, ZENGRC (Sept. 21, 2024), <https://www.zengrc.com/blog/navigating-the-future-of-ai-governance-a-guide-to-nist-ai-rmf-iso-iec-42001-and-the-eu-ai-act/> [<https://perma.cc/W48N-QWTJ>].

132. See AI Act, *supra* note 59.

coordinating audits and certification, and facilitating industry compliance within the boundaries set by EU law.

International standards such as ISO/IEC 42001, released jointly by the International Organization for Standardization and the International Electrotechnical Commission in December 2023, could serve as shared technical scaffolding across both jurisdictions.¹³³ ISO/IEC 42001 provides a voluntary certifiable framework for establishing and maintaining an AI management system; however, as a cross-sector management standard, it does not itself impose regulatory enforcement mechanisms or prescribe biometric-specific requirements.¹³⁴ In this respect, international standards would promote procedural consistency, while jurisdiction-specific SROs, anchored in NIST in the United States and the EU AI Act in the European Union, would supply the institutional enforcement, accountability, and legal alignment necessary for credible governance. For biometric AI, this combination would offer a practical mechanism to address recognized AI risks such as bias, data provenance, transparency, and misuse.¹³⁵

II. COMPARATIVE ANALYSIS OF REGIMES

A. Grading the European Union and the United States

A comparative evaluation of the EU's *ex ante* regulatory approach, the United States' *ex post* liability-driven model, and industry self-regulatory frameworks reveals that each system reflects distinct normative commitments and governance philosophies. The EU prioritizes precaution and fundamental rights, while the United States prioritizes innovation, market dynamism, and litigation-based deterrence. In contrast, self-regulatory models prioritize flexibility, rapid adaptation, and coordination among private actors.

133. See Sofia Bednarz & Susan Bennett, *AI Risks, Failures and Consequences: Corporate Governance for the AI Era*, 40 AUSTL. J. CORP. L. 39 (2025).

134. See ISO/IEC 42001:2023, *Information Technology—Artificial Intelligence—Management System* §§ 4.4, 6.1.1 (2023).

135. See Reto P. Grubenmann, *ISO/IEC 42001: A New Standard for AI Governance*, KPMG, <https://kpmg.com/ch/en/insights/artificial-intelligence/iso-iec-42001.html> [https://perma.cc/R5BC-NM8X] (last visited Nov. 18, 2025).

This section evaluates the regimes across three analytical dimensions: (1) Individual rights protection, (2) incentives for innovation, and (3) enforcement and accountability, highlighting their respective systemic strengths and weaknesses. These criteria map the core trade-offs at the heart of biometric AI governance: the tension between strong individual rights protections and the need to sustain technological progress. Evaluating each regime through this lens requires a deeper articulation of what each dimension captures and why it matters for systems built on inherently sensitive and immutable data.

Individual rights protection concerns the extent to which a governance system safeguards individuals from the unique risks posed by biometric technologies.¹³⁶ Key considerations include privacy and autonomy protections, transparency obligations, enforceable consent, limits on collection and repurposing. In the biometric context, consumer protection is therefore not merely a procedural safeguard, but a structural prerequisite for preserving trust and preventing irreversible harms.¹³⁷

Innovation incentives reflect the degree to which a regulatory environment supports experimentation, competition, and the iterative development of biometric AI technologies.¹³⁸ Effective systems balance flexibility and proportionality, allowing lower-risk applications to proceed with manageable compliance burdens while imposing stricter controls on high-risk or socially consequential uses.¹³⁹ Mechanisms such as regulatory sandboxes, risk-tiered regulation, and predictable approval pathways influence the pace of innovation as well as who gets to innovate, new entrants or dominant incumbents.¹⁴⁰

Enforcement and accountability concern the mechanisms that ensure compliance and provide meaningful remedies for violations.¹⁴¹ This may take the form of proactive audits, supervisory oversight, private rights of action, administrative

136. See generally González Fuster & Nadolna Peeters, *supra* note 46.

137. See *id.*

138. Kevin A. Bryan & Florenta Teodoridis, *Balancing Market Innovation Incentives and Regulation in AI: Challenges and Opportunities*, BROOKINGS (Sept. 24, 2024), <https://www.brookings.edu/articles/balancing-market-innovation-incentives-and-regulation-in-ai-challenges-and-opportunities/> [https://perma.cc/7ZNL-9ATP].

139. See *id.*

140. See *id.*

141. AI Act, *supra* note 59.

penalties, or industry-based certification systems. In the biometric context, where harms can propagate instantaneously and irreversibly, effective enforcement capacity is critical to the credibility of a governance regime.

1. Individual Rights Protection

i. The European Union

The EU AI Act's risk-based framework incorporates extensive consumer safeguards for AI systems, with particularly robust protections in place for biometric data. The legislation imposes transparency obligations on both providers and deployers of AI systems, including those performing emotion recognition or biometric categorization.¹⁴²

Transparency under the Act requires AI systems to be designed and used in a way that enables traceability between the input and the output and a clear explanation of how the system functions.¹⁴³ Because transparency and other obligations vary according to an AI system's assigned risk level, determining the applicable requirements should be identified on a case-by-case analysis with attention on the specific circumstances of deployment.¹⁴⁴ Biometric systems, when used for purposes other than verifying that a person is who they claim to be, are classified as high-risk under Annex III and Article 6(2), even when such use is permitted by relevant EU or national laws.¹⁴⁵ This high-risk characterization triggers mandatory conformity assessments (Article 43), post-market monitoring (Article 72), human oversight requirements (Article 14), and transparency (Article 13) of AI use, which collectively enhance consumer protection.

The EU's proactive approach aims to build public trust in AI technologies by safeguarding users' rights and well-being.¹⁴⁶ By prioritizing data security, privacy, and risk management, the EU

142. AI Act, *supra* note 59, art. 3. Providers are entities that develop or place AI systems on the market under their own name or trademark. Deployers are entities that use AI systems in a professional capacity—including with respect to systems performing emotion recognition or biometric categorization. *See id.*

143. *See id.*

144. *See id.*

145. *See id.* annex III (listing the high-risk AI systems referred to in Article 6(2)).

146. *See id.*

seeks to reassure the public that AI can be deployed safely and ethically.¹⁴⁷ This focus on responsible development helps to promote broader acceptance and integration of AI technologies, ultimately benefiting society as a whole.¹⁴⁸ Moreover, the EU AI Act is not merely a technical regulatory instrument; it is designed as an ethical framework intended to ensure that organizations consider the impact of their AI systems on individuals, other businesses, the environment, and broader social contexts.¹⁴⁹

Despite these strengths, critics argue that such regulations placed on providers of high-risk systems fail to promote the European Commission's stated goal of delivering a high level of protection for fundamental rights.¹⁵⁰ The discretion left to providers, combined with the structure of existing enforcement standards and available remedies, creates concerns that the EU's framework lacks the necessary scrutiny and oversight to ensure sufficient protection against the dangers that AI systems pose.¹⁵¹ More specifically, the provisions governing high-risk AI systems have been criticized for failing to prevent both actual and anticipated harms, including fundamental rights violations.¹⁵²

Commentators note that the Act leaves too much discretion to providers on sensitive and politically charged matters, a problem linked to an underlying misalignment between the Act's technical risk framework and the normative content of fundamental rights.¹⁵³ Requirements regarding data governance, transparency, and human oversight are described as ambiguous, fragmented, and

147. *See id.*

148. *See* BIRD & BIRD, EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT: A GUIDE 4 (2025), <https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf> [<https://perma.cc/AM6L-Y572>].

149. *See id.* at 3.

150. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (Apr. 21, 2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> [<https://perma.cc/C2N7-7QBE>].

151. *See* Nathalie Smuha et al., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act* (LEADS Lab, Univ. of Birmingham, Aug. 5, 2021), <https://ssrn.com/abstract=3899991> [<https://perma.cc/ZE53-L77G>].

152. *See id.* at 35.

153. *See id.*

confusing.¹⁵⁴ For example, although the Act requires high-risk systems to be sufficiently transparent for users to interpret and meaningfully employ system outputs, users are not obligated to communicate that information to persons subject to the AI-supported decision.¹⁵⁵ Nor must users explain or justify the decisions made with AI assistance to those affected by them.¹⁵⁶ The users' only explicit obligation toward affected persons is merely to inform them that an AI system is being used.¹⁵⁷

This market-oriented approach to fundamental rights falls short of the European Commission's intention of a "balanced and proportionate approach limited to the minimum requirements to address the risks linked to AI."¹⁵⁸ The thresholds for determining "acceptable" levels of AI risk before products enter the market are insufficient to ensure that AI providers respect fundamental rights.¹⁵⁹ By regulating AI systems through a product-safety paradigm, similar to cars, machinery, or toys, the Act overlooks the distinct societal implications of AI misuse.¹⁶⁰

Rather than prohibiting all AI systems that may infringe on fundamental rights, the Act targets only those that create an "unacceptable risk."¹⁶¹ As a result, AI systems that may still interfere with individual rights can remain permissible so long as providers comply with measures such as a voluntary code of conduct, enhanced transparency, or internal self-assessment.¹⁶² In contrast, only systems designated as "high risk" are subject to mandatory compliance obligations.¹⁶³ Consumer protection therefore largely depends on how the European Commission defines and updates the scope of high-risk systems, particularly for applications that affect large populations or limit meaningful

154. *See id.*

155. *See* Jean Joseph, *Should the United States Adopt Federal Artificial Intelligence Regulation Similar to the European Union?*, 20 LOY. U. CHI. INT'L L. REV. 105, 114 (2023).

156. *See id.*

157. *See id.*

158. *See* Natascha Gerlach, *The Case of the EU AI Act: Why We Need to Return to a Risk-Based Approach*, INT'L ASS'N OF PRIV. PROS. (Mar. 23, 2023), <https://iapp.org/news/a/the-case-of-the-eu-ai-act-why-we-need-to-return-to-a-risk-based-approach/> [<https://perma.cc/Z65T-LJV5>].

159. *See* Joseph, *supra* note 155, at 114.

160. *See id.*

161. *See id.* at 90.

162. *See id.* at 114.

163. *See id.*

opportunities to opt out.¹⁶⁴ Given the rapid pace of AI development, maintaining an accurate and forward-looking classification of high-risk systems presents a persistent challenge. Providers may be incentivized to reclassify or restructure systems to fall outside high-risk categories, potentially undermining the practical reach and effectiveness of the Act's mandatory safeguards.¹⁶⁵ In conclusion, while the EU regime represents the most structured and formalized consumer protection framework among the existing biometric regulation regimes, its practical effectiveness and full normative reach remain in transition.

ii. The United States

As noted, the United States lacks a single, comprehensive federal statute specifically governing biometric AI systems. Consumer protection instead relies on a patchwork of sectoral privacy laws, anti-discrimination statutes, and prohibitions on unfair or deceptive practices, enforced principally by the FTC, while supplemented by state-level biometric and privacy regulations.¹⁶⁶

One strength of the American model, particularly on the state side, is its institutional proximity to the affected constituencies.¹⁶⁷ State biometric information privacy laws often explicitly aim to safeguard individuals' highly sensitive identifiers, and state legislatures, being closer to local political and cultural preferences, can tailor rules to community priorities surrounding surveillance, workplace monitoring, and commercial tracking.¹⁶⁸ This localized structure can enable faster legislative responses where biometric misuse becomes salient within a particular state, whereas a comprehensive federal statute might subordinate more protective state approaches to national uniformity.¹⁶⁹

164. *See id.*

165. *See id.* at 115.

166. *See* Ariana Naranjo, *U.S. Biometric Data Laws*, TCW GLOBAL (Apr. 1, 2025), <https://www.tcwglobal.com/blog/u.s.-biometric-data-law> [https://perma.cc/D8CW-Y5VM] (citing FTC Biometric Policy Statement, *supra* note 92).

167. Haley Rubin, *It's My Data and I'll Protect It If I Want To: A Proposal to Standardize Biometric Data Privacy Laws Between the United States and European Union*, 58 VAND. J. TRANSNAT'L L. 261, 281–82 (2025).

168. *See id.*

169. *See id.*

At the federal level, this *ex post* model provides a different kind of flexibility. Even without a dedicated biometric-AI statute, the FTC has repeatedly affirmed its commitment to addressing unfair or deceptive practices related to the collection and use of consumers' biometric information under its broad Section 5 authority.¹⁷⁰ In particular, the FTC's 2023 Policy Statement on Biometric Information interprets Section 5 as reaching a non-exhaustive set of deceptive and unfair practices, including false or unsubstantiated marketing claims and misleading statements concerning the use of biometric data.¹⁷¹ The Statement also articulates affirmative expectations firms should implement, such as robust data security, vendor oversight, and ongoing monitoring of biometric systems to ensure they function as represented and do not cause foreseeable harm, particularly to vulnerable or historically marginalized groups.¹⁷² Collectively, this broad, technology-neutral authority allows regulators to map emerging biometric-AI harms onto existing unfair or deceptive practices frameworks, without awaiting new statutory enactments—giving the US regime a degree of adaptive enforcement capacity that can respond to novel biometric risks as they arise.¹⁷³

At the same time, the limits of the *ex post* model reveal systemic weaknesses in consumer protection. Commentators note that the FTC's reliance on its unfairness authority is constrained by the statutory requirement that an "unfair" practice cause or be likely to cause substantial injury that is not reasonably avoidable and not outweighed by countervailing benefits.¹⁷⁴ While the FTC's Statement provides an extensive discussion of potential harms and consumer unavoidability, it does not fully engage with the cost-benefit analysis required by the statute.¹⁷⁵ As a result of this

170. See Press Release, Fed. Trade Comm'n, FTC Warns About Misuses of Biometric Information and Harm to Consumers (May 18, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers> [https://perma.cc/ZTE3-4JCF].

171. See Jon Frankel, Steve Lane & Kandi Parsons, *FTC Warns About Misuses of Consumers' Biometric Information*, ZWILLGEN BLOG (June 1, 2023), <https://www.zwillgen.com/ftc-state-ag/ftc-warns-about-misuses-of-consumers-biometric-information/> [https://perma.cc/7ECM-V5CH].

172. See *id.*

173. See generally *id.*

174. See John Burroughs, *Twin Inadequacies in the FTC's Recent Biometrics Policy Statement*, 3 U. CHI. BUS. L. REV. 497, 500 (2024).

175. See *id.*

omission, enforcement may continue to gravitate toward deception cases, where firms can often insulate themselves against liability through expansive disclosures.¹⁷⁶

Increased disclosure will be of little benefit to consumers, as severe information asymmetries make it difficult for individuals to meaningfully assess the risks associated with providing their biometric information.¹⁷⁷ Moreover, the harms stemming from biometric misuse, such as data breaches leading to security vulnerabilities, are nearly impossible to rectify after the fact.¹⁷⁸ These characteristics underscore the need for a more proactive regulatory regime capable of preventing harm before it occurs.¹⁷⁹ For these reasons, a regime that intervenes primarily after injury will be ill-suited to mitigating the most serious biometric risks.¹⁸⁰

More broadly, the federal posture remains fundamentally reactive.¹⁸¹ Enforcement often follows a complaint, investigation, or public controversy, rather than preceding deployment or any type of preemptive oversight.¹⁸² Harm must often occur, or be credibly alleged, before agencies intervene.¹⁸³ This reactive orientation aligns with persistent public concern: survey data reveals that eighty-one percent of adults in the United States feel they lack control over data collected by companies, illustrating a widespread perception that existing protections fall short of constituent expectations.¹⁸⁴ The slow pace of federal privacy reform has further eroded trust in both corporate and governmental uses of biometric information, raising cross-border

176. *See id.* at 515.

177. *See id.* at 500.

178. *See id.* at 500–01.

179. *See id.* at 501.

180. *See id.* at 500–01.

181. *See* *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Katz v. United States*, 389 U.S. 347 (1967). *See generally* Press Release, H. Comm. on Oversight & Gov't Reform, Hearing Wrap Up: U.S. Federal Agencies Need Proactive Cybersecurity Strategy to Counter State-Sponsored Threats (Apr. 2, 2025), <https://oversight.house.gov/release/hearing-wrap-up-u-s-federal-agencies-need-proactive-cybersecurity-strategy-to-counter-state-sponsored-threats/> [https://perma.cc/9BBW-UUYV].

182. *See, e.g.*, Complaint for Permanent Injunction and Other Relief ¶¶ 22–24, 30–31, 42–74, *FTC v. Rite Aid Corp.*, No. 2:23-cv-05023 (E.D. Pa. Dec. 19, 2023); *see also* FTC Biometric Policy Statement, *supra* note 92, at 1–2.

183. *See, e.g.*, *FTC v. Rite Aid Corp.*, No. 2:23-cv-05023 (E.D. Pa. Dec. 19, 2023).

184. *See* Rubin, *supra* note 167, at 282.

concerns for consumers interacting with multinational firms subject to divergent privacy standards.¹⁸⁵

Although the US Constitution does not expressly guarantee a right to privacy, the Supreme Court has recognized privacy protections through several constitutional doctrines, including the substantive due process right recognized in *Griswold v. Connecticut* and the Fourth Amendment protections articulated in *Katz v. United States*. The scope of unenumerated constitutional rights, however, remains contested.¹⁸⁶ Most recently, in *Dobbs v. Jackson Women's Health Organization*, the Court emphasized that rights not expressly mentioned in the Constitution must be deeply rooted in the Nation's history and tradition to receive protection under the Fourteenth Amendment's Due Process Clause.¹⁸⁷ Against this backdrop of limited and fragmented federal constitutional protection, statutory safeguards have become particularly important in addressing emerging privacy concerns such as the collection and use of biometric information. Yet only a handful of states have enacted laws specifically protecting biometric information, leaving most Americans' biometric data largely unregulated and exposing individuals to significant vulnerabilities.¹⁸⁸ This fragmented landscape amplifies disparities: while some states offer robust biometric protections and, in some cases, private rights of action, a majority of others rely solely on general privacy or unfair-practices laws—frameworks that provide uncertain and often weaker deterrence.¹⁸⁹ As a result, coverage is uneven. Residents of states without biometric-specific laws face heightened exposure to the risks of expanding biometric data collection, cybercrimes, and pervasive digital transactions.¹⁹⁰

Regulatory fragmentation also complicates compliance for firms operating nationally, making it challenging to ensure uniform consumer rights across jurisdictions.¹⁹¹ Comparative scholarly analyses reinforce the picture that, although the United States is

185. *See id.* at 266.

186. *See id.*

187. *See Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 231 (2022).

188. *See id.* at 264.

189. *See id.*; *see also* Greg Marcus, *Wear Your Heart on Your Sleeve, Whether You Like It or Not: How Federal Regulation Can Address Advances in Biometric Technology*, 33 U. MIAMI BUS. L. REV. 131, 154 (2024).

190. *See Marcus, supra* note 189, at 152.

191. *See id.* at 156.

one of the most intensive users of biometric technologies, particularly for surveillance and authentication, it lacks comprehensive biometric privacy legislation, creating an asymmetry that heightens the potential for consumer harm.¹⁹² In conclusion, the US *ex post* model provides relatively dynamic and flexible tools for addressing biometric-AI harms; however, its reactive, fragmented, and disclosure-dependent structure lacks the comprehensive, preventative orientation of the EU framework, leaving critical biometric-AI risks unresolved.

2. Incentives for Innovation

i. The European Union

The EU AI Act establishes a unified legal framework across all twenty-seven Member States of the European Union, significantly reducing cross-border legal uncertainty for developers of biometric identification, biometric categorization, emotion recognition, and other AI systems.¹⁹³ By classifying many biometric applications as high risk, the Act replaces conflicting national approaches with harmonized standards applicable throughout the Single Market.¹⁹⁴ This regulatory uniformity enables firms to design, deploy, and scale AI products across the EU without navigating divergent national compliance regimes, thereby supporting innovation through legal certainty even as substantive safeguards are imposed.¹⁹⁵

Through its differentiated risk tiers, the Act provides developers with clearer expectations regarding transparency, safety, and data-management obligations applicable to each category of AI system, thereby reducing regulatory uncertainty at the design stage.¹⁹⁶ This framework is embedded within a broader EU ecosystem that is expressly oriented toward fostering

192. *See id.* at 141.

193. *See AI Act*, EUR. COMM'N, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> [<https://perma.cc/KYZ7-6L62>] (last visited Oct. 29, 2025) [hereinafter *AI Innovation Package*].

194. *See id.*

195. *See id.*

196. *See id.*; *see also* European Commission Press Release IP/24/383, Commission Launches AI Innovation Package to Support Artificial Intelligence Startups and SMEs (Jan. 23, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383 [<https://perma.cc/BS45-A7KF>].

trustworthy AI.¹⁹⁷ This ecosystem includes initiatives such as the AI Innovation Package, the deployment of AI Factories to support experimentation, and the establishment of the AI Office to coordinate AI governance and enforcement across Member States.¹⁹⁸ Collectively, these initiatives aim to strike a balance between safety, protection of fundamental rights, and human-centric AI, while also promoting uptake, investment, and innovation throughout the EU.¹⁹⁹

Article 40(3) of the Act expressly requires participants in AI standardization processes to promote investment and innovation, primarily by enhancing legal certainty and supporting competitive market conditions.²⁰⁰ This provision reflects the EU's broader ambition to treat standardization as more than a constraint on innovation, instead viewing it as a mechanism for converting regulatory predictability into a strategic advantage.²⁰¹ This standardization strategy is reinforced by complementary policy measures aimed at lowering structural barriers to AI innovation, particularly for startups and small and medium-sized enterprises (SMEs).²⁰² The AI Innovation Package targets the high compliance and infrastructure costs that have historically limited participation in regulated AI markets.²⁰³ A central component of this effort is the amendment of the EuroHPC Regulation to establish AI Factories as new pillars of the EU's supercomputing ecosystem.²⁰⁴ AI Factories are designed to acquire and operate AI-dedicated supercomputers, provide startups and SMEs with broad access to high-performance computing resources, and function as one-stop hubs for algorithmic development, testing, and validation.²⁰⁵ By expanding access to advanced computational infrastructure, these initiatives strengthen European technological sovereignty, enabling smaller

197. See European Commission Press Release IP/24/383, *supra* note 196.

198. See *id.*

199. See *id.*

200. AI Act, *supra* note 59, art. 40.

201. See *AI Innovation Package*, *supra* note 193.

202. See *AI Innovation Package*, *supra* note 193.

203. See *id.*

204. See *EuroHPC JU's Mandate Expanded Under New Regulation Amendment*, EUR. HIGH-PERFORMANCE COMPUTING JOINT UNDERTAKING (Jan. 20, 2026), https://www.eurohpc-ju.europa.eu/eurohpc-jus-mandate-expanded-under-new-regulation-amendment-2026-01-20_en [<https://perma.cc/776Y-R2JF>].

205. *AI Innovation Package*, *supra* note 193.

firms to compete more effectively with global technology incumbents.²⁰⁶

The EU's AI Start-Up and Innovation Communication further expands financial and human capital support measures, intending to generate approximately four billion euros in public and private investment by 2027.²⁰⁷ Funding of this scale supports the development of generative and large-scale AI, strengthening the EU's generative AI talent pipeline through training and reskilling programs, expanding access to venture capital and equity financing, and advancing Common European Data Spaces that provide developers with high-quality, interoperable datasets for responsible model training.²⁰⁸ The GenAI4EU initiative similarly seeks to stimulate new AI use cases across Europe's fourteen industrial ecosystems and key public sector domains, from robotics and biotechnology to virtual worlds, health, manufacturing, climate technologies, and mobility.²⁰⁹ Together, these programs integrate ethical oversight with industrial policy, anchoring the EU's strategy for achieving global competitiveness in trustworthy AI.

Complementing these investment-focused efforts, the European Commission published a comprehensive 135-page set of guidelines to promote the consistent and uniform application of the EU AI Act across the EU.²¹⁰ Although non-binding, these guidelines offer essential insights into the Commission's interpretations of various provisions, including prohibitions, legal definitions, and operational requirements, accompanied by practical examples.²¹¹ Once again, the EU reaffirms its commitment to fostering a safe, reliable, and ethical AI landscape.²¹² Some legal scholars go further, arguing that such regulatory clarity in a highly specialized domain supports trust-driven innovation by giving

206. *See id.*

207. *AI Innovation Package*, *supra* note 193.

208. *See id.*

209. *See id.*

210. *Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act*, EUR. COMM'N (Feb. 4, 2025), <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> [<https://perma.cc/SVM2-7V8Y>].

211. *See id.*

212. *See id.*

consumers confidence in AI products and encouraging support for market participants.²¹³

However, despite its innovation-oriented architecture, the EU's *ex ante* bureaucracy imposes high costs, many of which are not yet fully quantifiable.²¹⁴ Critics contend that these obligations will deter investment in European AI startups, slow the digitization of the economy, and drive entrepreneurial talent to jurisdictions with fewer procedural hurdles.²¹⁵ These concerns are intensified by the EU AI Act's expansive extraterritorial reach, applying to all companies—regardless of whether they maintain a physical presence or operations within the EU—that develop, supply, manufacture, market, or offer biometric systems for use in the EU, or that deploy systems generating outputs used within the EU.²¹⁶ As a result, a broad range of global companies will need to adapt to the EU's comprehensive regulatory scheme, irrespective of their primary market focus or operational geography.²¹⁷

As of October 2025, reports from industry trade groups indicate that the European technology sector is already experiencing slower growth among local AI startups, leaving them trailing behind US competitors with fewer regulatory constraints.²¹⁸ Nearly sixty percent of small European technology companies reported delays in product development due to

213. See Kevin Frazier, *Clear Rules, Bold Innovation: Finding the Regulatory Sweet Spot for AI*, YALE J. ON REGUL. (Apr. 6, 2025), <https://www.yalejreg.com/nc/clear-rules-bold-innovation-finding-the-regulatory-sweet-spot-for-ai-by-kevin-frazier/> [https://perma.cc/Z9Y2-G463].

214. See Benjamin Mueller, *How Much Will the Artificial Intelligence Act Cost Europe?*, CTR. DATA INNOVATION (July 26, 2021), <https://www2.datainnovation.org/2021-ai-a-costs.pdf> [https://perma.cc/V6SC-5HJX].

215. See *id.*

216. See David J. Oberly, *Analyzing the EU Artificial Intelligence Act: Spotlight on Biometrics*, BAKER DONELSON (May 16, 2024), <https://www.bakerdonelson.com/analyzing-the-eu-artificial-intelligence-act-spotlight-on-biometrics> [https://perma.cc/VL5A-4BHU].

217. See *id.*

218. See Rachyl Jones, *Europe's AI Rules Slow Tech Startups While US Speeds Ahead, Report Finds*, SEMAFOR (Oct. 9, 2025), <https://www.semafor.com/article/10/09/2025/europes-ai-rules-slow-tech-startups-while-us-speeds-ahead-report-finds> [https://perma.cc/5NUW-BYNJ]; see also *79% of Tech Founders Hit by Regulatory Friction as EU Simplification Grinds to a Halt in Brussels, New Research Finds*, COMPUT. & COMM'NS INDUS. ASS'N (July 1, 2026), <https://ccianet.org/news/2026/07/79-of-tech-founders-hit-by-regulatory-friction-as-eu-simplification-grinds-to-a-halt-in-brussels-new-research-finds/> [https://perma.cc/6AEU-QTRT] (reporting that 79% of surveyed EU tech founders experienced significant regulatory friction, including delayed market entry, paused or cancelled product features, and delayed or lost deals).

regulatory burdens, compared to forty-four percent of small US companies.²¹⁹ Such delays are compounded by functional compromises: one-third of European developers at small companies removed or downgraded product features, predominantly those related to data handling and safety checks to comply with the Act, while sixty percent acknowledged that they had not yet adapted their systems and remained uncertain about future compliance.²²⁰ In other words, European startups report significantly lower confidence than US startups in their ability to meet upcoming regulatory expectations.

Economists have also raised concerns that the EU's increasingly progressive regulatory posture fails to fully account for potential drawbacks, particularly the unpredictable evolution of machine-learning methods.²²¹ They warn that the Act risks "freezing innovation in a framework built for yesterday's technology," especially as European firms already lag behind American and Chinese competitors.²²² Instead of securing leadership in trustworthy AI, the EU may inadvertently widen the innovation gap, creating a market where advancement is slower and less contested.²²³ Despite the EU's otherwise supportive ecosystem, the EU AI Act standardization process remains incomplete and AI standards are currently immature relative to those in other heavily regulated sectors, such as aviation or pharmaceuticals.²²⁴ This immaturity may increase compliance costs and lead to inconsistent enforcement, thereby undermining the EU's goal of achieving "legal certainty that promotes innovation."²²⁵

219. See Jones, *supra* note 218.

220. See *id.*

221. See Thibault Schrepel, *Pauses Will Not Fix the European Union's AI Act*, REGUL. REV. (Nov. 3, 2025), <https://www.theregreview.org/2025/11/03/schrepel-pauses-will-not-fix-the-european-unions-ai-act/> [<https://perma.cc/3CRT-FDLD>].

222. See *id.*

223. See *id.*

224. See Hadrien Pouget & Ranj Zuhdi, *AI and Product Safety Standards Under the EU AI Act*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Mar. 5, 2024), <https://carnegieendowment.org/research/2024/03/ai-and-product-safety-standards-under-the-eu-ai-act?lang=en> [<https://perma.cc/2K6U-5C7K>].

225. See *id.*

ii. The United States

From an innovation standpoint, the United States has long been an attractive jurisdiction for companies developing and deploying cutting-edge biometric-AI technologies, largely because it lacks the rigid *ex ante* constraints characteristic of the EU. The absence of a comprehensive federal AI or biometric-privacy statute allows firms to experiment, iterate, and commercialize rapidly, without undergoing pre-deployment conformity assessments or extensive regulatory vetting. This permissive environment enables industries to test biometric applications, often in real-world settings, without the delays associated with formal authorization. For instance, in the retail sector, companies increasingly view the difficult trade-off between biometric innovation and privacy compliance as a manageable risk in exchange for competitive market advantages.²²⁶ Many retailers tailor biometric tools such as facial recognition or palm-scanning checkout systems to appeal to privacy-conscious consumers and employees, effectively designing their own internal “best practices” to balance personalization with procedural safeguards.²²⁷

Significantly, some companies are innovating in privacy-preserving design itself. One biometric-AI company, for example, transforms raw biometric data into mathematical hash files at the moment of capture, eliminating the storage of biometric templates altogether.²²⁸ By doing so, this process produces a non-biometric, irreversible “unique output” capable of verifying identity but incapable of being reverse-engineered into the original biometric sample.²²⁹ This form of privacy engineering demonstrates how market incentives can drive technical innovation in both biometric performance and privacy protection, without relying on regulatory mandates.²³⁰ The regulatory lightness of the American approach

226. See Bailey White, *Tailoring Biometric Innovation to Privacy Law in the Retail Industry*, 27 SMU SCI. & TECH. L. REV. 343, 373 (2024).

227. See *id.*

228. See *id.*

229. See *id.*

230. See generally Russ Banham, *Two Global Marketplaces, Two AI Approaches*, LEADER'S EDGE (Oct. 31, 2025), <https://www.leadersedge.com/industry/two-global-marketplaces-two-ai-approaches> [https://perma.cc/2WTY-AERF].

subconsciously encourages firms to experiment aggressively and adapt quickly, contributing to a fast-paced innovation cycle.²³¹

However, this flexibility comes at the cost of coherence. The absence of unified federal standards has produced a complex regulatory landscape, which many commentators identify as a growing threat to US innovation and global competitiveness in biometric technology.²³² The existing patchwork of laws and regulations introduces compliance uncertainty and legal risk, raising barriers to long-term investment and complicating nationwide product deployment.²³³ Commentators argue that a unified federal privacy and biometric framework would mitigate wasteful and unnecessary compliance overhead, providing clearer expectations for developers.²³⁴

A consolidated federal standard, they contend, would incentivize modernization within corporate IT and security teams, improving data governance, cybersecurity resilience, and ethical AI practices.²³⁵ Instead, the current landscape forces companies to engineer bespoke compliance strategies for different jurisdictions, diverting resources away from research, model improvement, and privacy-by-design innovation.²³⁶ Without uniform expectations for data retention, deletion, purpose limitation, and transparency, firms face uncertainty about what constitutes adequate protection in biometric-AI development, which slows innovation at the architectural level.²³⁷

This decentralized system also undermines consumer trust, which is critical for widespread adoption of biometric technologies.²³⁸ Frequent data breaches, coupled with inconsistent breach notification requirements across states, make it difficult for consumers to assess which entities are trustworthy.²³⁹ Eroding public confidence, stemming from uneven accountability

231. *Id.*

232. Marcus, *supra* note 189, at 153.

233. *See id.*

234. *See* Yaki Faitelson, *Why U.S. GDPR-Style Laws Are Good for Business*, FORBES (Dec. 19, 2019), <https://www.forbes.com/councils/forbestechcouncil/2019/12/19/why-u-s-gdpr-style-privacy-laws-are-good-for-business/> [<https://perma.cc/UGE6-Q4Z9>].

235. *See id.*

236. *See id.*

237. *See id.*

238. *See id.*

239. *See id.*

frameworks, has direct economic consequences, including a lower willingness to share biometric data, reluctance of enterprise partners to integrate third-party biometric tools, and an overall chilling effect on investment in technologies that rely on sensitive identifiers.²⁴⁰

At the other extreme of the regulatory landscape, certain state-level laws, most prominently BIPA, illustrate the risks of concentrated over-deterrence. BIPA's strict liability structure and statutory damages, combined with its private right of action, have incentivized extensive litigation.²⁴¹ While effective at encouraging compliance, BIPA has generated significant litigation anxiety, particularly among smaller startups and small and medium-sized firms.²⁴² Even minor technical lapses in notice, retention schedules, or data handling can trigger class actions seeking millions of dollars in damages.²⁴³ This litigation risk has led some companies to scale back or abandon biometric deployments altogether, despite potential benefits in authentication security, fraud prevention, accessibility tools, and customer personalization.²⁴⁴

In short, the US system exhibits a dual imbalance: under-regulation at the federal level produces uncertainty, inefficiency, and inconsistent expectations. At the same time, over-regulation in certain states creates punitive liability environments that deter experimentation. The result is an innovation landscape marked by rapid progress, but constrained stability. Biometric AI innovation in the United States is fast, adaptive, and market-driven, yet also reactive, fragmented, and structurally fragile.

3. Enforcement, Regulatory Effectiveness & Accountability

i. The European Union

The EU AI Act establishes a hybrid enforcement regime that combines centralized and decentralized oversight through a layered institutional architecture governing the full lifecycle of

240. *See generally id.*

241. Marcus, *supra* note 189, at 153.

242. *See id.*

243. *See id.*

244. *See id.*

risky AI technologies, including biometric systems.²⁴⁵ Strategic guidance is provided by three advisory bodies: the European Artificial Intelligence Board, the Scientific Panel, and the Advisory Forum.²⁴⁶ Effective enforcement authority, however, rests with the European AI Office, established within the European Commission, and national market surveillance authorities (MSAs)—which are responsible for implementing, supervising, and enforcing the Act.²⁴⁷

At the national level, Member States therefore play a pivotal role, because each must designate at least one notifying authority and at least one MSA to function as national competent authorities (“Notifying Authorities”).²⁴⁸ Notifying Authorities are responsible for appointing and supervising notified bodies, which are independent entities tasked with conducting pre-market conformity assessments of high-risk AI systems.²⁴⁹ Once an AI system is placed on the market, put into service, or used within a Member State’s jurisdiction, MSAs assume responsibility for post-market supervision.²⁵⁰ Acting pursuant to Regulation (EU) 2019/1020, MSAs possess robust investigative and corrective powers, including the authority to conduct remote monitoring, access providers’ technical documentation, datasets, source code, and impose sanctions.²⁵¹ They may also initiate joint investigations

245. See Catherine Di Lorenzo et al., *Zooming in on AI—#14: Enforcement of the AI Act*, A&O SHEARMAN (Feb. 4, 2025), <https://www.aoshearman.com/en/insights/aoshearman-on-tech/zooming-in-on-ai-14-enforcement-of-the-ai-act> [https://perma.cc/XZS5-PFLD].

246. See *Governance and Enforcement of the AI Act*, EUR. COMM’N (Aug. 7, 2026), <https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement> [https://perma.cc/A5V7-PPHC] (describing how the European Artificial Intelligence Board coordinates Member State authorities and promotes consistent implementation of the Act; the Scientific Panel provides independent expert advice concerning general-purpose AI models, systemic risks, classification, evaluation, and market surveillance; and the Advisory Forum provides stakeholder expertise and advice on implementation, standardization, and related issues).

247. See *Governance and Enforcement of the AI Act*, *supra* note 246.

248. See *id.*

249. See *id.*

250. See *Market Surveillance Authorities Under the AI Act*, EUR. COMM’N (Sept. 26, 2025), <https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act> [https://perma.cc/4A3X-798S].

251. Regulation (EU) 2019/1020, of the European Parliament and of the Council of 20 June 2019 on Market Surveillance and Compliance of Products, 2019 O.J. (L 169) 1.

with the Commission, request corrective measures, and levy penalties where necessary.²⁵²

The AI Office introduces a novel layer of centralized oversight to this framework. It is empowered to coordinate enforcement actions, conduct investigations, and directly supervise general-purpose AI (GPAI) systems and high-risk biometric applications.²⁵³ Acting on behalf of the Commission, the AI Office may initiate proceedings on its own initiative in response to complaints from downstream providers and follow qualified alerts issued by the Scientific Panel.²⁵⁴ Beyond its coordination function, the AI Office can exercise direct investigative and corrective powers over GPAI providers—including the authority to request documentation and information, conduct model evaluations to assess compliance and systemic risk, and require the implementation of corrective measures.²⁵⁵ Where non-compliance persists, the Commission may impose fines of up to €15 million or three percent of total worldwide annual turnover, whichever is higher.²⁵⁶ The AI Office may also intervene at the request of MSAs where cross-border coordination or specialized expertise is required.²⁵⁷

The Act reinforces enforcement through substantial sanctioning authority at the national level. MSAs may impose administrative fines calibrated to the severity of the infringement: up to the greater of €35 million or seven percent of global annual turnover for prohibited AI practices; the greater of €15 million or three percent for breaches of core obligations applicable to operators of high-risk systems; and the greater of €7 million or one percent for supplying incorrect, incomplete, or misleading information to authorities.²⁵⁸

In parallel, the Act establishes an unusually broad right of complaint. Any person with grounds to suspect a violation may submit a complaint to the relevant MSA, regardless of whether they are personally affected by the AI system in question.²⁵⁹ While this expansive standing is intended to facilitate detection and oversight

252. *See id.*

253. *See Governance and Enforcement of the AI Act, supra* note 246.

254. *See* Di Lorenzo et al., *supra* note 245.

255. *See id.*

256. *See id.*

257. *See id.*

258. *See id.*

259. *See id.*

of systemic risks, it also raises concerns about strategic or abusive complaints.²⁶⁰

Finally, cooperation and coordination mechanisms further strengthen enforcement. Where an MSA determines that non-compliance extends beyond national borders, it must notify the Commission and other Member States, share its findings, and communicate the corrective measures required of the operator.²⁶¹ If adequate remedies are not implemented within the prescribed timeframe, the MSA must adopt provisional measures that restrict or suspend the system's availability or use and notify the Commission and other Member States.²⁶² Such measures are deemed automatically justified unless objections are raised within three months for high-risk AI systems, or thirty days for prohibited practices.²⁶³

Taken together, this accessible multilevel governance framework, combining centralized oversight, decentralized enforcement, severe financial penalties, and broad complaint rights, provides multiple mechanisms through which abusive biometric uses, such as unconsented facial scraping or emotion-recognition surveillance, will be detected, investigated, and sanctioned.

However, despite its ambition, legal scholarship increasingly argues that the AI Act's enforcement framework, while theoretically optimistic, is overly complex in practice.²⁶⁴ More specifically, critics argue that the administrative burdens and uneven application create tension among relevant parties.²⁶⁵ A central critique is the absence of a "one-stop-shop" mechanism.²⁶⁶ Unlike the GDPR's lead-supervisory-authority system, the AI Act may require operators to interact with multiple authorities across different Member States, depending on where their systems are

260. *See id.*

261. *See id.*

262. *See id.*

263. *See id.*

264. *See id.*

265. *See id.*

266. *See* HANS GRAUX ET AL., INTERPLAY BETWEEN THE AI ACT AND THE EU DIGITAL LEGISLATIVE FRAMEWORK 22 (Eur. Parl., Directorate-Gen. for Internal Pol'y, Oct. 2025), [https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU\(2025\)778575_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf) [<https://perma.cc/87J9-TRDL>].

marketed, deployed, or used.²⁶⁷ Although the Act establishes cooperation mechanisms among competent authorities, its multi-authority enforcement structure may itself create administrative inefficiencies by requiring authorities to coordinate overlapping investigations, exchange information across jurisdictions, and determine which authority bears responsibility for particular enforcement actions. These additional layers may delay investigations and undermine some of the efficiency that the Act's cooperation mechanisms seek to achieve. The administrative burden of dealing with multiple authorities may prove burdensome and arguably negates prospective efficiency.²⁶⁸

Enforcement uniformity is further threatened by procedural divergence among Member States. The Act does not specify deadlines for authorities to act, limitation periods, complainants' rights to be heard or to access the investigation file, or requirements for authorities to publish their decisions.²⁶⁹ These procedural elements fall instead under national law, resulting in significant variability.²⁷⁰ From a substantive standpoint, Member States retain discretion over which agency becomes the MSA; some Member States may rely on existing data protection authorities (DPAs), while others may create new, specialized bodies specifically for this purpose, ultimately producing varying levels of expertise.²⁷¹ Due to this discretion, institutional culture and resource allocation are likely to lead to divergent interpretations and enforcement approaches.²⁷² Early academic analysis warns that, echoing the difficulties in GDPR enforcement, these differences in national administrative procedures, cooperation mechanisms, and institutional capacity among the MSAs will likely lead to inconsistent interpretations of the law.²⁷³ The Commission has already proposed a separate Regulation to harmonize aspects

267. See Di Lorenzo et al., *supra* note 245.

268. See *id.*

269. See *id.*

270. See *id.*

271. See *id.*

272. See *id.*

273. See Stella (Ziyu) Zhou, *From Data Processing to Artificial Intelligence: The Evolution of EU Technology Enforcement Under the GDPR and the AI Act* (Stanford-Vienna Transatlantic Tech. L.F., EU L. Working Paper No. 118, 2025), <https://law.stanford.edu/wp-content/uploads/2025/06/EU-Law-WP-118-Zhou.pdf> [<https://perma.cc/9H2Q-SRTU>].

of GDPR enforcement, illustrating the ongoing difficulty of coordinating enforcement across Member States.²⁷⁴

The overlap with the GDPR and the broader digital regulatory landscape creates additional uncertainty. For biometric AI, the EU AI Act sits on top of the GDPR, the Law Enforcement Directive, the Data Act, the DSA/DMA, and sector-specific rules.²⁷⁵ A 2025 European Parliament study found that, while each individual EU legislative and regulatory instrument is “well-targeted” individually, their interplay creates significant regulatory complexity with overlaps and gaps that are objectively more complex with new governance innovations.²⁷⁶ Identifying which obligations apply to a given AI system and how they interact often requires specialized legal and technical expertise beyond the reach of many stakeholders.²⁷⁷

Therefore, despite the image of comprehensive organization, the resulting landscape is highly fragmented. A single legal framework rarely governs AI systems, nor will it be governed by the interpretations of a single supervisor or regulator.²⁷⁸ An AI service provider seeking to offer its services across the EU market will need to familiarize itself with multiple legal frameworks at both the EU and national levels, as well as with the opinions and interpretations of authorities that can differ amongst Member States and economic sectors.²⁷⁹ Since these authorities have different policy priorities, there is a clear risk of contradiction and tension between positions.²⁸⁰

Finally, timing and resource constraints may leave a window where “bad” systems slip through. Member States were required to designate national competent authorities by August 2, 2025.²⁸¹ Following subsequent amendments to the Act’s implementation

274. See Di Lorenzo et al., *supra* note 245.

275. See Graux et al., *supra* note 266, at 22.

276. See *id.*

277. See *id.* at 13.

278. See *id.* at 78.

279. See *id.* at 79.

280. See *id.*

281. See *id.* at 10; see also Benjamin W. Perry & Justin T. Tarka, *Cybersecurity Awareness Month in Focus, Part III: The EU AI Act Is Here—What It Means for U.S. Employers*, OGLETREE DEAKINS (Oct. 31, 2025), <https://ogletree.com/insights-resources/blog-posts/cybersecurity-awareness-month-in-focus-part-iii-the-eu-ai-act-is-here-what-it-means-for-u-s-employers/> [https://perma.cc/GVU3-2FFG].

timeline, requirements for high-risk AI systems generally apply beginning December 2, 2027, while requirements for high-risk AI systems embedded in regulated products apply beginning August 2, 2028.²⁸² During this transition period, harmful biometric-AI systems may remain outside the Act's full high-risk compliance regime, while providers and deployers must prepare for obligations whose practical implementation continues to depend in part on forthcoming guidance and harmonized standards.²⁸³

In conclusion, the EU, on paper, has established one of the strongest enforcement regimes in the world for biometric AI. GDPR precedent demonstrates that EU authorities can impose substantial penalties, order deletion of unlawfully collected biometric data, and send clear signals against uses that contravene public policy.²⁸⁴ The EU AI Act further includes *ex ante* controls, GPAI oversight, and extensive new fining powers. Yet, the system's multilayered structure creates substantial compliance complexity, while divergent national implementation may lead to uneven enforcement. The resulting uncertainty and regulatory burden risk over-detering or delaying beneficial biometric-AI applications, including privacy-preserving identity tools and accessibility technologies.

282. See *Navigating the AI Act*, EUR. COMM'N, <https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act> [<https://perma.cc/YY2B-9F8U>] (last visited Aug. 8, 2026) (explaining that AI Act governance rules became applicable on August 2, 2025, high-risk AI system requirements apply beginning December 2, 2027, and requirements for AI systems embedded in regulated physical products apply beginning August 2, 2028).

283. See Pieter Haeck & Gabriel Gavin, *EU Prepares to Delay Landmark AI Rules by One Year*, POLITICO (Nov. 13, 2025), <https://www.politico.eu/article/eu-to-propose-delay-of-key-part-of-landmark-ai-law-by-one-year/> [<https://perma.cc/6ZVV-QYZK>].

284. See, e.g., *Facial Recognition: Clearview AI Fined €20 Million and Ordered to Stop Processing Data of Individuals in France*, CNIL (Oct. 20, 2022), <https://www.cnil.fr/en/facial-recognition-clearview-ai-fined-20-million-euros-and-ordered-stop-processing-data> [<https://perma.cc/S2EW-MH23>]; see also *Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million*, EUR. DATA PROT. BD. (Mar. 10, 2022), https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en [<https://perma.cc/2MXL-9RAT>]; *Imposition of Fine on Clearview AI, Inc.*, HELLENIC DATA PROT. AUTH. (July 13, 2022), <https://www.dpa.gr/en/en/enimerwtiko/prakseisArxis/imposition-fine-clearview-ai-inc> [<https://perma.cc/3PHE-QHEU>]; *Dutch DPA Imposes a Fine on Clearview Because of Illegal Data Collection for Facial Recognition*, AUTORITEIT PERSOONSGEGEVENS (Sept. 3, 2024), <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition> [<https://perma.cc/9F72-Q22Y>].

ii. The United States

The US enforcement model is characterized by a flexible agency authority that enables regulators to respond rapidly to emerging harms in biometric AI systems. Rather than relying on *ex ante* approval regimes, US agencies apply existing statutory authority to novel technologies through *ex post* enforcement. The FTC, for example, has explicitly extended its consumer protection mandate to biometric information technologies. In 2023, the FTC issued a policy statement warning companies that unfair or deceptive practices involving biometric-AI fall squarely within the scope of Section 5 of the FTC Act.²⁸⁵ The statement clarified that longstanding consumer protection principles apply to emerging biometric systems, reducing ambiguity about the federal capability to regulate these types of processes.²⁸⁶

The FTC further articulated a set of non-exhaustive factors it would consider when evaluating whether a company's use of biometric information or biometric-AI constitutes an unfair practice.²⁸⁷ This framework operates as a flexible, technology-neutral enforcement tool applicable across all technologies, allowing the FTC to adapt oversight to new biometric use cases without waiting for new legislation—a catch-all approach.²⁸⁸ Relevant factors include: failures to assess foreseeable consumer harms prior to data collection; failures to mitigate known or foreseeable risks; surreptitious or unexpected collection or use of biometric information; inadequate vetting of third-party vendors or affiliates; insufficient employee training; and the absence of ongoing monitoring to ensure that biometric technologies function as intended without harming consumers.²⁸⁹

This *ex-post* structure also supports rapid innovation and experimentation. Since firms do not face pre-deployment approvals for biometric-AI tools, they can deploy systems quickly, refine them through real-world use, and correct them later if concerns arise.²⁹⁰ When problems emerge, regulators can rely on

285. See Frankel et al., *supra* note 171.

286. See *id.*

287. See *id.*

288. See *id.*

289. See *id.*

290. See Anthony E. DiResta & Zachary Sherman, *The FTC Is Regulating AI: A Comprehensive Analysis*, HOLLAND & KNIGHT LLP (July 25, 2023), <https://www.hklaw.com/>

broadly framed enforcement tools, particularly Section 5 of the FTC Act, to intervene without delay.²⁹¹ This approach leverages existing statutory authority to address biometric misuse as it arises, rather than depending on bespoke biometric-AI statutes.²⁹²

The presence of multiple regulatory actors and jurisdictions further reinforces accountability.²⁹³ In addition to the FTC, other federal agencies, state regulators, and private litigants play roles in monitoring biometric-AI practices, increasing the probability that abuses will be detected.²⁹⁴ Some agencies, such as the Consumer Financial Protection Bureau, the Equal Employment Opportunity Commission (EEOC), the Departments of Health and Human Services, Justice, Education, Homeland Security, and Labor, have pledged to apply their existing statutory authorities to promote fairness, equality, and justice as AI technologies proliferate across sectors.²⁹⁵ The EEOC's AI and Algorithmic Fairness Initiative exemplifies this approach, ensuring that these technologies comply with federal civil rights laws by guiding the use of AI in job decisions—thereby mitigating discrimination and bias in automated systems.²⁹⁶

Despite these advantages, the US system's reliance on *ex post* enforcement means that regulatory intervention often occurs only after harm has already materialized.²⁹⁷ Companies and consumers frequently learn the practical contours of biometric-AI compliance through litigation outcomes, settlements, or consent decrees, often years after deployment.²⁹⁸ High-profile cases involving companies

en/insights/publications/2023/07/the-ftc-is-regulating-ai-a-comprehensive-analysis [https://perma.cc/UU6A-JSP8].

291. *See id.*

292. *See id.*

293. *See* Tatevik Davtyan, *The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained*, 16 J.L. TECH. & INTERNET 223, 254 (2024).

294. *See* Kirk Nahra et al., *Biometric Privacy as a Case Study for U.S. Privacy Overall*, TECHREG CHRON., Apr. 2024, at 3, 8, <https://www.privacysecurityacademy.com/wp-content/uploads/2024/10/20240429-CPI-Biometric-Privacy-as-a-Case-Study-for-US-Privacy-Overall.pdf> [https://perma.cc/R53Q-SMTP].

295. *See id.*

296. *See id.*

297. *See* Talia Gillis, Scott Nelson & Jann Spiess, *Regulating Algorithms: What and When*, in REGULATING ARTIFICIAL INTELLIGENCE 6 (Nat'l Bureau of Econ. Rsch., preliminary draft, May 31, 2025), <https://www.nber.org/system/files/chapters/c15123/c15123.pdf> [https://perma.cc/BAP3-MLZN].

298. *See* Maurice Wells, *Biometric Backlash: The Rising Wave of Litigation Under BIPA and Beyond*, EPSTEIN BECKER GREEN P.C. (Aug. 21, 2025), <https://www.>

such as Meta or Amazon illustrate how potentially harmful biometric practices may persist for extended periods before regulators intervene.²⁹⁹ During this time, consumer rights may already be compromised, and remediation may come too late to prevent widespread harm.³⁰⁰ This lag is particularly concerning given the pace of technological development. A 2024 report by the National Academies of Sciences, Engineering, and Medicine observed that facial-recognition technologies in the United States are “outpacing laws and regulations,” underscoring the risk that enforcement will perpetually trail innovation.³⁰¹

State-by-state enforcement further fragments the regulatory landscape. Although private rights of action enhance accountability, they also generate uneven compliance burdens and legal uncertainty.³⁰² Firms deploying biometric-AI nationally must navigate divergent state standards, exposing them to over-deterrence in some jurisdictions while leaving gaps in protection in others.³⁰³ This fragmentation complicates scaling and discourages the deployment of legitimate biometric innovations—particularly among smaller firms with limited legal resources.³⁰⁴ A related structural weakness arises from the design of specific state biometric privacy laws, particularly those that impose statutory damages.³⁰⁵ Under BIPA, for example, technical violations such as failing to publish a data-retention schedule or obtain written consent may trigger the same statutory penalties as substantive

commerciallitigationupdate.com/biometric-backlash-the-rising-wave-of-litigation-under-bipa-and-beyond [https://perma.cc/2RUA-GRSC].

299. See *Recent Lawsuits Against AI Companies: Beyond Copyright Infringement*, TRAVERSE LEGAL (May 19, 2025), <https://www.traverselegal.com/blog/ai-litigation-beyond-copyright/> [https://perma.cc/AFL7-DGF3].

300. See generally Press Release, Fed. Trade Comm’n, *supra* note 170.

301. See Josh Blatt, *Advances in Facial Recognition Technology Have Outpaced Laws, Regulations; New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns*, NAT’L ACADS. OF SCIS., ENG’G & MED. (Jan. 17, 2024), <https://www.nationalacademies.org/news/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns> [https://perma.cc/JBY4-Z3MB].

302. See Anna L. Metzger, *The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy*, 50 LOY. U. CHI. L.J. 1051, 1091–97 (2019).

303. See Amanda Reid, *The Mathematics of Regulatory Fragmentation: Understanding the Multiplicative Costs of State-Level Platform Requirements*, 15 IP THEORY 24, 76 (2025).

304. See *id.* at 68–69.

305. See Marcus, *supra* note 189, at 158.

privacy harms.³⁰⁶ This lack of proportionality can distort enforcement incentives, punishing minor procedural lapses as harshly as “egregious misuse,” thereby creating significant litigation risk—even for well-intentioned firms.³⁰⁷

The scalability of enforcement also presents challenges. Oversight responsibilities are dispersed across numerous agencies and jurisdictions, while biometric-AI systems—especially those deployed at scale in public or commercial settings—generate vast volumes of data and involve substantial technical complexity.³⁰⁸ Regulators may lack the necessary resources or expertise to monitor all relevant deployments effectively.³⁰⁹ This constraint risks selective or inconsistent enforcement, further undermining predictability.

In conclusion, the US *ex post* enforcement regime offers speed, flexibility, and adaptability—encouraging rapid innovation and swift regulatory responses when biometric-AI harms are identified. However, the absence of firm pre-market controls allows risky systems to be deployed before their societal impacts are fully understood. Fragmented oversight, uneven standards, and delayed intervention can erode consumer trust and lead to underdeterrence of harmful practices. While the system excels at reacting to misuse, it remains less effective at preventing it and creates a landscape in which biometric-AI innovation advances quickly but often at the cost of stability, proportionality, and sustained public confidence.

B. Applied Case Studies: Comparative Illustrations

To move beyond abstract regulatory models and assess how biometric AI governance operates in practice, this Section examines a series of applied case studies across distinct functional domains: identity authentication and user verification, deepfake detection and content authentication, iterative AI training and consent, and law enforcement-driven mass identification. By juxtaposing US and EU responses to real-world deployments of

306. *See id.* at 144.

307. *See id.* at 146, 158.

308. *See* Oksana Meier, *AI Regulations in the United States*, PACIFIC AI (Nov. 13, 2025), <https://pacific.ai/ai-regulations-in-the-us/> [<https://perma.cc/5PLT-MQCU>].

309. *See id.*

major technology firms, this analysis illustrates how divergent governance architectures shape consumer protection, innovation incentives, and regulatory effectiveness.

1. Identity Authentication and User Verification: United States Response to Meta

Meta's reintroduction of facial recognition for identity verification provides a clear illustration of how the US biometric governance regime operates through *ex post* enforcement. Although Meta implemented internal privacy controls and framed facial recognition as a tool for account recovery and fraud prevention, its deployment continued to expose the company to significant liability, particularly under Illinois' BIPA, for collecting facial geometry data without explicit, informed consent.³¹⁰ This dynamic highlights both the deterrent power of private litigation and the inefficiency of a system in which compliance standards are learned primarily through lawsuits.

Meta's early facial recognition initiatives triggered two record-breaking enforcement actions that reshaped the legal and commercial landscape for biometric AI in the United States.³¹¹ In *In re Facebook Biometric Information Privacy Litigation*, a class action alleging that Facebook's "Tag Suggestions" feature collected and analyzed users' facial templates without the notice and consent required by BIPA ultimately resulted in a \$650 million settlement.³¹² This case marked one of the largest biometric privacy settlements in US history, demonstrating the extraordinary financial exposure associated with procedural noncompliance.³¹³ Meta's consequences only intensified further in 2024, when Texas secured a \$1.4 billion settlement under CUBI for the same facial recognition practices.³¹⁴ Unlike the 2021 litigation, which private plaintiffs drove, the Texas action was brought directly by the state, positioning it as an aggressive public enforcer of biometric privacy rights.³¹⁵ The unprecedented size of the

310. See Lesley Rice Montgomery, *Facebook and the Biometric Information Privacy Act Litigation*, 13 J. NEW MEMBERS ROUND TABLE 71, 75 (2025).

311. See *id.*

312. See *id.*

313. See *id.*

314. See *Recent Lawsuits Against AI Companies*, *supra* note 299.

315. See *id.*

settlement sent an unmistakable signal to the technology sector: failure to obtain informed consent for biometric data collection can result in multibillion-dollar liability.³¹⁶ Together, these cases reshaped Meta's corporate risk calculus and signaled to industry peers that, in the US, the risk of litigation can function as a *de facto* regulatory ban on certain biometric uses.³¹⁷ Rather than prohibiting facial recognition outright through legislation, the cumulative threat of class actions, statutory damages, and state enforcement has effectively rendered the technology commercially untenable at scale.

Following the \$650 million settlement and amid mounting regulatory scrutiny, Meta announced the shutdown of its global Face Recognition system in late 2021.³¹⁸ The company acknowledged that facial recognition offered tangible benefits, such as fraud prevention, accessibility for the visually impaired, and automated user tagging, but conceded that its long-term role in society required broader public deliberation and more explicit regulatory norms.³¹⁹ As Meta explained:

Every new technology brings with it potential for both benefit and concern, and we want to find the right balance. In the case of facial recognition, its long-term role in society needs to be debated openly, among those who will be most impacted by it. We will continue engaging in that conversation and working with the civil society groups and regulators who are leading this discussion.³²⁰

This episode highlights a defining characteristic of the US *ex post* model: procedural compliance, even in the absence of demonstrated concrete consumer harm, can trigger existential liability through statutory damages and class actions. While this enforcement mechanism powerfully deters abusive biometric practices, it does so through retroactive punishment rather than

316. *See id.*

317. *See Meta's Facial Recognition Lawsuit Underscores Enforcement Risk*, BLOOMBERG L. (Feb. 15, 2022), <https://news.bloomberglaw.com/privacy-and-data-security/metatexas-facial-recognition-suit-shows-enforcement-headache> [<https://perma.cc/G4K4-FWAE>].

318. *See* Jerome Pesenti, *An Update on Our Use of Face Recognition*, META NEWSROOM (Nov. 2, 2021), <https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/> [<https://perma.cc/73UC-JB5P>].

319. *See id.*

320. *See id.*

through prospective clarity, often forcing firms to abandon entire categories of innovation after costly legal battles, rather than shaping safer deployment *ex ante*.

2. Deepfake Detection and Content Authentication: EU Response to Meta

In 2025, Meta expanded facial-recognition identity verification using short video selfies in the United Kingdom, the European Union, and South Korea.³²¹ The system enables users to record a brief selfie video to verify account ownership and combat deepfake-based, so-called “celeb-bait” scams, in which malicious actors misuse images of public figures to promote fraudulent advertisements or redirect users to deceptive websites.³²² Under this process, Meta compares the face appearing in advertisements to images it holds for verified public figures.³²³ When a match is detected, the system confirms through the public figure’s profile whether the ad is legitimate and endorsed.³²⁴

The feature incorporates several design constraints aimed at minimizing biometric risk. Participation is strictly opt-in, biometric data is deleted immediately after verification, and no persistent facial templates are retained.³²⁵ These safeguards reflect alignment with core GDPR principles—including data minimization, explicit consent, and purpose limitation under Articles 5, 6, and 9,³²⁶ and largely anticipate the EU AI Act’s heightened scrutiny of biometric systems used for identity verification and content authentication.

Crucially, before deployment, Meta engaged in informal consultations with EU data protection authorities, adopting a *de facto* pre-clearance approach characteristic of the EU’s *ex ante*,

321. See *Testing New Ways to Combat Scams and Help Restore Access to Compromised Accounts*, META (Oct. 21, 2024), <https://about.fb.com/news/2024/10/testing-combat-scams-restore-compromised-accounts/> [<https://perma.cc/Q862-F6EJ>].

322. See *id.*

323. See *id.*

324. See *id.*

325. See *id.*

326. See generally Felipe Romero-Moreno, *Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights*, 58 COMPUT. L. & SEC. REV. 106162 (2025), <https://doi.org/10.1016/j.clsr.2025.106162> [<https://perma.cc/Q6TC-7GXL>].

cooperative regulatory style.³²⁷ This engagement provided conditional regulatory assurance that the system complied with existing GDPR obligations and was likely to align with forthcoming EU AI Act obligations governing high-risk biometric applications.³²⁸ The episode illustrates how the EU framework channels biometric-AI innovation through structured dialogue and anticipatory compliance, emphasizing harm prevention and legal certainty over rapid deployment.

This case study stands in sharp contrast with the US litigation-driven approach. Whereas the American system relies on *ex post* deterrence through massive liability exposure, the EU model seeks to shape biometric-AI design upstream by embedding safeguards before harm occurs. More broadly, the EU's risk-based regulatory framework is designed to anticipate deepfake-related harms. As discussed previously, AI-driven content authentication and identity verification systems involving biometric processing are presumptively considered "high-risk" under the EU AI Act, triggering *ex ante* compliance obligations before these systems can be placed on the market.³²⁹

3. Iterative AI Training and Consent: The BIPA Response to Amazon

Amazon's biometric privacy litigation in Illinois illustrates how litigation-as-regulation exposes the structural limits of *ex post* governance for AI systems that rely on iterative training. At the center of this controversy is Amazon's facial-recognition ecosystem. Amazon Rekognition is marketed for law enforcement, security, and commercial analytics, while Amazon Photos serves as a consumer-facing image-storage platform.³³⁰ Plaintiffs alleged that Amazon covertly scanned and analyzed facial geometries from user-uploaded photos on Amazon Photos to train and refine Rekognition's algorithms, which Amazon then licenses to third parties—including police departments and enterprise clients—without obtaining the written, informed consent required by

327. See *DPC Statement on Meta AI*, DATA PROT. COMM'N (May 21, 2025), <https://www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai> [<https://perma.cc/MTJ7-9JRZ>].

328. See *id.*

329. See AI Act, *supra* note 59.

330. See *Recent Lawsuits Against AI Companies*, *supra* note 299.

BIPA.³³¹ These claims reveal a procedural paradox: even an AI system, when framed as protective or efficiency-enhancing, may trigger strict liability when formal consent mechanisms are absent.

i. Illinois BIPA Class Action: Amazon Photos and Rekognition

In May 2021, plaintiffs filed *B.H. v. Amazon.com Inc.* in the Northern District of Illinois, alleging that Amazon violated and continues to violate BIPA.³³² The suit, brought on behalf of a minor plaintiff, claims that Amazon Photos secretly collected, scanned, stored, and analyzed facial geometries of individuals appearing in user-uploaded photos using Rekognition.³³³ These practices allegedly occurred regardless of whether the individuals were Amazon customers or had provided consent to the processing.³³⁴

Plaintiffs contend that Amazon uses these biometric scans to train Rekognition's AI models, thereby improving the system's accuracy and commercial value while profiting from the biometric identifiers of millions of users.³³⁵ This conduct, plaintiffs argued, constitutes the unlawful use of biometric data for profit, directly contravening BIPA §§ 15(b)–(e), which require companies to obtain written, informed consent before collection and to maintain reasonable data-retention and destruction policies.³³⁶ The complaint further alleges that Amazon improperly shifted compliance burdens onto users by stating that Illinois law *may* require users themselves to obtain consent from individuals appearing in their photos.³³⁷ Plaintiffs argue that this obligation properly belongs to Amazon, not the consumer, given its control over the underlying AI system and downstream data use.³³⁸ They

331. *See id.*

332. *See B.H. v. Amazon.com, Inc.*, No. 1:21-cv-02617 (N.D. Ill. Mar. 30, 2022).

333. *See id.*

334. *See Amazon May Be Unlawfully Using Its Facial Recognition Technology*, LOWE & ASSOCs., <https://lowelaw.com/amazon-may-be-unlawfully-using-its-facial-recognition-technology/> [<https://perma.cc/9QAH-FEJN>] (last visited Mar. 10, 2026).

335. *See* Corrado Rizzi, *Amazon Hit with Class Action Over Alleged Use of Ill. Residents' Facial Scans to Improve, Market Rekognition Tech*, CLASSACTION.ORG (May 18, 2021), <https://www.classaction.org/news/amazon-hit-with-class-action-over-alleged-use-of-ill.-residents-facial-scans-to-improve-market-rekognition-tech> [<https://perma.cc/LV6V-ANH9>].

336. *See id.*

337. *See Amazon May Be Unlawfully Using Its Facial Recognition Technology*, *supra* note 334.

338. *See id.*

also note that image-recognition features could be enabled with minimal user interaction, effectively encouraging participation without adequate notice or understanding of consent requirements.³³⁹

Critically, the alleged practices extend beyond Amazon's direct customers.³⁴⁰ Anyone whose image appears in an uploaded photo, even if they are not a user with a contractual relationship with Amazon, may be included in the class.³⁴¹ Given that approximately 5.8 million Amazon Prime users reside in Illinois, aggregate statutory damages (ranging from \$1,000 to \$5,000 per violation) could reach into the billions.³⁴² *B.H. v. Amazon.com Inc.* remains ongoing and critically underscores a core tension in AI governance: while iterative training is vital for algorithmic improvement, using biometric data for that purpose without explicit consent constitutes a statutory violation under current state law.³⁴³

ii. COVID-19 Workplace Data and AWS Liability

A separate 2023 class action further illustrates the breadth of BIPA exposure, extending beyond consumer-facing biometric systems to employment and workplace health-screening contexts. In *Trio v. Amazon Web Services*, the plaintiff filed suit in the Circuit Court of Cook County, Illinois, alleging that Amazon Web Services (AWS) unlawfully collected, stored, and processed facial geometry data obtained through COVID-19 workplace screenings conducted via third-party "Turing Shield" devices.³⁴⁴ Trio claims she was

339. See Rizzi, *supra* note 335.

340. See *id.*

341. See *id.*

342. See *id.*; see also *The Class Action Weekly Wire—Episode 128: Illinois Federal Judge Certifies Class of 1.2 Million Amazon Alexa Users in BIPA Class Action*, DUANE MORRIS CLASS ACTION DEF. BLOG (Nov. 26, 2025), <https://blogs.duanemorris.com/classactiondefense/2025/11/26/the-class-action-weekly-wire-episode-128-illinois-federal-judge-certifies-class-of-1-2-million-amazon-alexa-users-in-bipa-class-action/> [https://perma.cc/2T3W-FJVU].

343. Publicly available records reviewed through March 2026 do not indicate that the parties have reached a settlement in *B.H. v. Amazon.com Inc.*

344. *Trio v. Amazon Web Servs., Inc.*, No. 2023-CH-00544 (Ill. Cir. Ct. Cook Cnty. filed Jan. 19, 2023); see also *Amazon Class Action Alleges Company Collected, Stored Employee Data During COVID Screenings*, TOP CLASS ACTIONS (Jan. 27, 2023), <https://topclassactions.com/lawsuit-settlements/lawsuit-news/amazon-class-action-lawsuit-and-settlement->

required to submit to a facial scan each time she began her shift as part of a mandatory COVID-19 screening protocol.³⁴⁵

As detailed in the complaint, Turing Shield kiosks utilize built-in thermal sensors to measure forehead temperature and facial recognition software to assess mask compliance.³⁴⁶ During this process, the devices capture and analyze workers' facial geometry, which is then stored in a database hosted by AWS.³⁴⁷ Trio alleges that Turing contracted with Amazon for both cloud storage and software services, including Amazon's Rekognition.³⁴⁸ As a result, AWS allegedly retained biometric data collected through these screenings and used it to enhance its own capabilities and those of its "affiliated machine-learning and artificial intelligence technologies," without obtaining consent or providing notice.³⁴⁹

Plaintiffs argue that Amazon's biometric data collection violates multiple provisions of BIPA.³⁵⁰ Specifically, the complaint alleges that AWS failed to obtain prior written consent before collecting or storing biometric identifiers, to disclose the specific purpose and duration of data use, to maintain a publicly available retention and destruction schedule, and unlawfully disclosed biometric identifiers to third parties and affiliated entities without authorization.³⁵¹ The suit emphasizes that AWS allegedly shifted the benefits of biometric collection toward improving and commercializing its AI technologies, thereby wrongfully profiting from the facial scans of non-consenting workers.³⁵²

Central to the plaintiff's claims is the irreversible nature of biometric harm.³⁵³ The complaint stresses that facial geometry

news/amazon-class-action-alleges-company-collected-stored-employee-data-during-covid-screenings/ [https://perma.cc/LGK6-HP4A].

345. See *Amazon Class Action Alleges Company Collected, Stored Employee Data During COVID Screenings*, *supra* note 344.

346. See Kelly Mehorter, *Amazon Web Services Hit with Class Action Over Alleged Collection of Turing Shield Users' Facial Scans*, CLASSACTION.ORG (Jan. 27, 2023), <https://www.classaction.org/news/amazon-web-services-hit-with-class-action-over-alleged-collection-of-turing-shield-users-facial-scans> [https://perma.cc/G5JT-RQ7Z].

347. See *id.*

348. Class Action Complaint at 3, *Trio v. Amazon Web Servs., Inc.*, No. 2023-CH-00544 (Ill. Cir. Ct. Cook Cnty. Jan. 19, 2023).

349. See *id.*

350. See *id.* at 6.

351. See *id.* at 12.

352. See *id.* at 3.

353. See generally *id.*

scans constitute a unique, permanent biometric identifier that cannot be changed or replaced if compromised.³⁵⁴ As such, AWS's alleged data practices exposed workers to "serious and irreversible privacy risks," subjecting plaintiffs to the risk of identity theft, unauthorized tracking, and secondary use in the event of a breach.³⁵⁵

The plaintiff seeks declaratory and injunctive relief, statutory damages, and a jury trial on behalf of a proposed class comprising all Illinois individuals whose facial geometry was "collected, captured, received, obtained, maintained, stored, used, and/or disclosed" by AWS through Turing Shield devices during the applicable limitations period.³⁵⁶ Notably, the litigation underscores the question of whether biometric-AI systems deployed in employment or workplace safety contexts are subject to the same procedural safeguards as consumer-facing technologies under BIPA. In this respect, the case illustrates how AI-driven data repurposing, particularly when embedded in ostensibly protective workplace technologies, may collide with strict consent-based biometric privacy regimes.³⁵⁷

iii. Broader Regulatory and Market Implications

Collectively, these lawsuits position Amazon as a repeat target for BIPA enforcement, emblematic of how corporations may face liability not for demonstrable harm, but for procedural noncompliance, such as missing consent forms or insufficient notices. The absence of federal uniformity leaves multinational firms like Amazon navigating a regulatory vacuum punctuated by hyperactive state enforcement in only a handful of jurisdictions.

The outcome of these Illinois cases will likely set a precedent for whether AI companies can lawfully use user-generated content to train and improve models when that content contains biometric identifiers.³⁵⁸ If the courts side with the plaintiffs, companies may be forced to restructure data pipelines—segregating training data by jurisdiction—or abandon certain forms of model improvement

354. *See id.* at 4.

355. *See id.*

356. *See id.* at 15.

357. *See id.*

358. *See Recent Lawsuits Against AI Companies*, *supra* note 299.

altogether.³⁵⁹ Such rulings would have far-reaching consequences: heavy statutory penalties and class-action exposure may discourage iterative AI improvement within the US market; companies may relocate data processing operations offshore to avoid state-level exposure—exacerbating global data fragmentation and reducing domestic innovation.

The broader lesson from Amazon's cases is that litigation-driven enforcement creates a reactive compliance culture. Rather than fostering privacy by design, it pushes companies to contain liability retroactively. Amazon's exposure under BIPA and related suits reveals how procedural privacy law can yield substantive innovation consequences. In an environment without federal standards, companies face regulatory uncertainty, inconsistent enforcement, and a substantial risk of costly litigation.

4. Law Enforcement and Mass Identification: United States and EU Response to Clearview AI

The actions of Clearview AI represent one of the most controversial intersections of biometric data, AI innovation, and privacy law in recent years. Its unauthorized scraping of billions of facial images triggered coordinated enforcement actions across the European Union, the United Kingdom, Canada, and Australia, yet resulted in only sporadic and fragmented litigation in the United States.³⁶⁰ This episode exemplifies a fundamental philosophical divide: the EU prioritizes data-subject consent and extraterritorial accountability, while the US system privileges innovation, speech-based defenses, and *ex post* litigation.

Founded in 2017, Clearview develops facial recognition software primarily marketed to law enforcement agencies and select commercial clients.³⁶¹ Its proprietary system scrapes images from publicly accessible websites and social media platforms, extracting and indexing biometric facial geometry.³⁶² Users can upload a photo and instantly receive potential identity matches

359. *See id.*

360. *See About ClearviewAI's Mockery of Human Rights, Those Fighting It, and the Need for EU to Intervene*, EUR. DIGIT. RTS. (EDRI) (Apr. 6, 2022), <https://edri.org/our-work/we-need-to-talk-about-clearview-ai/> [<https://perma.cc/C34V-GJHN>].

361. *Clearview AI for Investigations*, CLEARVIEW AI, <https://www.clearview.ai/> [<https://perma.cc/4GR6-XT3J>] (last visited Sept. 21, 2025).

362. *See id.*

from Clearview's massive database.³⁶³ Estimates suggest that Clearview has collected as many as fifty billion images, creating one of the world's largest biometric repositories.³⁶⁴ Although the underlying images are publicly available, Clearview's algorithm transforms publicly available images into uniquely identifying biometric information, effectively enabling identification across the public internet without consent.³⁶⁵

i. United States Enforcement and Settlement Dynamics

In 2020, a New York Times exposé revealed the scope of Clearview's scraping—triggering dozens of lawsuits and enforcement actions in multiple jurisdictions.³⁶⁶ Eleven federal and state lawsuits were consolidated into *In re Clearview AI, Inc. Consumer Privacy Litigation*.³⁶⁷ Plaintiffs alleged that Clearview violated multiple state statutes, including BIPA, Virginia's unauthorized-use and computer-crimes laws, California's unfair-competition and privacy laws, and New York's invasion-of-privacy provisions. They also sought declaratory relief under the federal Declaratory Judgment Act.³⁶⁸ Under BIPA, plaintiffs asserted violations for collecting biometric data without written consent, profiting from biometric identifiers, unauthorized disclosure of data, and failure to implement proper retention and destruction policies.³⁶⁹

363. See Troutman Pepper Locke State Attorneys General Team et al., *\$51.75M Settlement in Clearview AI Biometric Privacy Litigation Illustrates Creative Resolution for Startups Facing Parallel Litigation and Enforcement Action*, TROUTMAN PEPPER LOCKE LLP (Apr. 30, 2025), <https://www.regulatoryoversight.com/2025/04/51-75m-settlement-in-clearview-ai-biometric-privacy-litigation-illustrates-creative-resolution-for-startups-facing-parallel-litigation-and-enforcement-action/> [https://perma.cc/ZHE3-8UTH].

364. Chris Burt, *Clearview Facial Recognition Searches Double, Database Reaches 50B Images*, BIOMETRIC UPDATE (June 26, 2024), <https://www.biometricupdate.com/202406/clearview-facial-recognition-searches-double-database-reaches-50b-images> [https://perma.cc/SD3U-3LY3].

365. See *id.*

366. See *id.*

367. *In re Clearview AI, Inc. Consumer Priv. Litig.*, No. 1:21-cv-00135 (N.D. Ill. Mar. 20, 2025); see also Nitzan Halperin et al., *A First in BIPA Litigation: Class Members Receive Equity in Clearview AI*, NAT'L L. REV. (July 22, 2025), <https://natlawreview.com/article/first-bipa-litigation-class-members-receive-equity-clearview-ai> [https://perma.cc/WW43-Q3U7].

368. See *\$51.75M Settlement in Clearview AI Biometric Privacy Litigation*, *supra* note 363.

369. See *id.*

Given BIPA's statutory damages of \$1,000 to \$5,000 per violation, and the potentially limitless class (any individual with an online image), a traditional damages award could have bankrupted the company.³⁷⁰ In March 2025, the court approved an unprecedented \$51.75 million settlement, granting the class a twenty-three percent equity stake in Clearview, payable upon one of four contingent liquidity events, such as an IPO, merger, liquidation, or buy-back option.³⁷¹ Individual members within the settlement class may choose whichever right to relief they believe is most advantageous as future events unfold.³⁷²

This equity-based settlement is unprecedented in privacy litigation, effectively tying class members' compensation to Clearview's commercial success and profitability.³⁷³ The more law enforcement agencies adopt its technology, the higher the plaintiffs' potential payout.³⁷⁴ Critics argue the deal undermines deterrence by transforming injured parties into stakeholders in the very technology they challenged.³⁷⁵ Twenty-three state attorneys general objected, warning that the agreement complicates future enforcement by creating a financial disincentive for additional oversight: any regulatory action that reduces Clearview's market share could simultaneously reduce the plaintiffs' recovery.³⁷⁶ The settlement thus reveals a structural paradox, demonstrating that litigation intended to punish unlawful biometric collection may end up institutionalizing it.

This paradox deepened through a separate settlement with the ACLU in Illinois in May 2022, which imposed a five-year nationwide injunction barring Clearview from serving private entities and Illinois agencies, but left its core business model intact by permitting continued sales to federal, state, and local law

370. See Halperin et al., *supra* note 367.

371. See *id.* Attorneys' fees were set at 39.1% of any realized equity. See *\$51.75M Settlement in Clearview AI Biometric Privacy Litigation*, *supra* note 363.

372. See generally *In re Clearview AI, Inc. Settlement*, CLEARVIEW CLASS ACTION, <https://clearviewclassaction.com/> [<https://perma.cc/S3G4-MM2K>] (last visited Mar. 12, 2026).

373. See Mike Scarcella, *U.S. Judge Approves "Novel" Clearview AI Class Action Settlement*, REUTERS (Mar. 21, 2025), <https://www.reuters.com/legal/litigation/us-judge-approves-novel-clearview-ai-class-action-settlement-2025-03-21/> [<https://perma.cc/X3TQ-J2PW>].

374. See *id.*

375. See Halperin et al., *supra* note 367.

376. See *id.*

enforcement agencies outside Illinois.³⁷⁷ Clearview admitted no liability and the settlement required no payment of damages to the plaintiffs; Clearview's only monetary payment was \$250,000 in attorneys' fees.³⁷⁸ As Clearview's counsel stated:

This settlement is a huge win for Clearview AI. Clearview will make no changes to its current business model, it will continue to expand its business offerings in compliance with applicable law and it will pay a small amount of money to cover advertising and fees, far less than continued litigation would cost.³⁷⁹

Together, these agreements produced a hybrid regulatory outcome that directly constrains the future oversight and investigative abilities of state attorneys general without fully prohibiting the challenged conduct. Clearview is legally restricted in certain jurisdictions but simultaneously remains economically incentivized to expand elsewhere. In essence, litigation intended to curb unlawful biometric collection instead risks institutionalizing it, displaying how procedural settlements can normalize invasive technologies by converting penalties into market legitimacy. This dynamic creates a structural incentive for enforcers to accept partial, jurisdiction-specific remedies over more comprehensive restrictions, even where the latter might better serve privacy protection goals.

Moreover, any multistate enforcement action imposing a broad geographic injunction would significantly reduce Clearview's potential revenue base, thereby diminishing the monetary relief available to plaintiffs.³⁸⁰ This arrangement places state attorneys general in a structural bind. Coordinated enforcement by the twenty-two objecting states could substantially curtail, if not effectively eliminate, Clearview's operations within their jurisdictions.³⁸¹ Yet, such collective action

377. *See Clearview AI Settles ACLU Illinois Lawsuit Confirming Continuity of Business Supporting Public Safety*, POLICE1 (Oct. 11, 2024), <https://www.police1.com/police-products/police-technology/police-software/facial-recognition/clearview-ai-settles-aclu-illinois-lawsuit-confirming-continuity-of-business-supporting-public-safety> [<https://perma.cc/LS2Q-WR42>].

378. *See id.*

379. *See id.*

380. *See \$51.75M Settlement in Clearview AI Biometric Privacy Litigation*, *supra* note 363.

381. *See Scarcella*, *supra* note 373.

would likely reduce the monetary recovery available to class plaintiffs, inviting further litigation and weakening incentives for aggressive injunctive relief.³⁸² Further compounding this tension is that many state and local agencies themselves rely on Clearview's technology—which makes robust enforcement politically and operationally costly.³⁸³ The result is a regulatory stalemate: Clearview operates under partial legal constraint while remaining commercially viable and positioned to expand in jurisdictions where enforcement pressure is less intense.

ii. The EU's GDPR Response to Clearview

Prior to the adoption of the EU AI Act, regulators across Europe initiated coordinated investigations into Clearview AI, citing violations of data protection principles under the GDPR and GDPR-analogous regimes.³⁸⁴ Multiple DPAs sanctioned Clearview for breaches of Articles 5, 6, 9, 12, 15, 17, and 31 of the GDPR, citing unlawful processing of biometric data, lack of transparency, and failure to cooperate with supervisory authorities.³⁸⁵

France's Commission Nationale de l'Informatique et des Libertés (CNIL) imposed a €20 million fine, and ordered the deletion of all data relating to French residents, finding violations of lawfulness (Art. 6), transparency (Arts. 12–14), and noncooperation (Art. 31).³⁸⁶ Italy's Garante issued a matching €20 million fine for unlawful processing of biometric data and failure to honor access and deletion requests.³⁸⁷ Greece's Hellenic DPA levied an additional €20 million fine and ordered the cessation of all processing involving Greek residents.³⁸⁸ The Dutch Supervisory

382. *See id.*

383. *See id.*

384. *See generally Challenge Against Clearview AI in Europe*, PRIV. INT'L, <https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe> [<https://perma.cc/XQY6-8X5P>] (last visited Mar. 11, 2026).

385. *See* Miriam Kohn, *Clearview AI, TikTok, and the Collection of Facial Images in International Law*, 23 CHI. J. INT'L L. 195, 211 (2022).

386. *See CNIL Issues €20 Million GDPR Fine to Clearview AI*, DATA PRIV. MANAGER (Oct. 21, 2022), <https://dataprivacymanager.net/cnil-issues-e20-million-gdpr-fine-to-clearview-ai/> [<https://perma.cc/6EWU-YBEU>].

387. *See Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million*, *supra* note 284.

388. *See Hellenic DPA Fines Clearview AI €20 Million*, EUR. DATA PROT. BD. (July 20, 2022), https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en [<https://perma.cc/YH52-3RND>].

Authority escalated enforcement in May 2024, issuing a €30.5 million fine, four cease-and-desist orders, and additional daily penalties for non-compliance—making it the largest EU sanction against Clearview to date.³⁸⁹ Collectively, these measures represent a pan-European condemnation of untargeted biometric scraping, treating the practice as a fundamental rights violation under the GDPR’s “special category data” regime. Clearview has nonetheless refused to comply or pay, arguing that it lacks an EU establishment and does not “offer goods or services” within the meaning of Article 3(2) GDPR.³⁹⁰

In the United Kingdom, whose post-Brexit data protection regime remains substantively aligned with the EU GDPR, enforcement initially stalled when the First-Tier Tribunal accepted Clearview’s claim that its data collection activities were conducted exclusively for foreign law enforcement purposes and therefore fell “beyond the material scope” of UK GDPR.³⁹¹ That interpretation was overturned in October 2025, when the Upper Tribunal held that Clearview’s mass collection of images of UK residents constitutes “monitoring of behavior” within the meaning of GDPR Article 3(2)(b), confirming that such cross-border biometric processing falls within domestic data protection jurisdiction.³⁹²

These jurisdictional disputes expose the limits of extraterritorial enforcement. While the GDPR clearly applies in

389. See *Dutch Supervisory Authority Imposes a Fine on Clearview Because of Illegal Data Collection for Facial Recognition*, EUR. DATA PROT. BD. (Sept. 3, 2024), https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en [<https://perma.cc/LF2N-SVKR>].

390. See *EU: Dutch Data Protection Fine Further Highlights Questions over Extra-Territorial Scope and International Enforceability of GDPR*, EVERSHEDES SUTHERLAND (Oct. 28, 2024), <https://www.eversheds-sutherland.com/en/finland/insights/eu-dutch-ddpa-clearview-ai-fine> [<https://perma.cc/Y63L-CY3W>].

391. *Clearview AI Inc. v. Info. Comm’r* [2023] UKFTT 819 (GRC); see also *Info. Comm’r’s Off. v. Clearview AI Inc.* [2025] UKUT 319 (AAC); Frank Hersey & Sam Clark, *Clearview AI Overturns UK Privacy Enforcement as Court Opens Questions on GDPR Jurisdiction*, MLEX (Oct. 17, 2023), <https://mlex.shorthandstories.com/clearview-ai-overturns-uk-privacy-enforcement-as-court-opens-questions-on-gdpr-jurisdiction/index.html> [<https://perma.cc/37UM-3TEG>].

392. See Edward Machin, *What the Latest Clearview AI Judgment Tells Us About Behavioural Monitoring and Big Data Under the GDPR*, ROPES & GRAY LLP (Oct. 15, 2025), <https://www.ropesgray.com/en/insights/viewpoints/102lq4y/what-the-latest-clearview-ai-judgment-tells-us-about-behavioural-monitoring-and-b> [<https://perma.cc/L6U3-NG9N>].

theory,³⁹³ practical enforcement against non-EU entities without assets or operational presence in Europe remains difficult.³⁹⁴ Significantly, the Clearview precedent marks an assertive extension of the GDPR's reach into AI-driven biometric scraping, signaling that "publicly available" no longer equates to "lawfully processable."³⁹⁵ The European approach thus contrasts sharply with US outcomes: while American litigation led to a financial settlement preserving Clearview, EU authorities imposed ongoing operational bans and deletion orders—even if collection remains unenforced outside their borders.

iii. Comparative Implications

The Clearview case highlights a profound gap in international privacy enforcement. Under US federal law, untargeted facial-image scraping remains largely permissible until a state-level lawsuit succeeds, whereas under the GDPR, comparable conduct is presumptively unlawful and subject to immediate administrative sanctions. However, neither system fully resolves the challenges posed by AI-scale biometric extraction.

In the United States, the Clearview case highlights the limitations of a reactive, litigation-driven approach to oversight in addressing systemic privacy violations enabled by AI. More broadly, the case demonstrates how the re-identification of publicly available data, once assumed to fall outside the scope of privacy law, now triggers statutory liability when combined with AI inference capabilities, yet remains subject to slow, fragmented, and unevenly distributed enforcement across jurisdictions.

393. As explicitly mentioned in Article 3(2) of the GDPR: "This regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: a. The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b. The monitoring of their behavior as far as their behavior takes place within the Union." GDPR, *supra* note 49, art. 3(2).

394. See generally JEAN HERVÉGUET ET AL., STUDY ON THE ENFORCEMENT OF GDPR OBLIGATIONS AGAINST ENTITIES ESTABLISHED OUTSIDE THE EEA BUT FALLING UNDER ARTICLE 3(2) GDPR (Eur. Data Prot. Bd., Nov. 2021), https://www.edpb.europa.eu/system/files/2023-04/call_9_final_report_04112021_en_0.pdf [<https://perma.cc/KKK6-ECJU>].

395. See Louise Brooks, *Data Scraping: How to Use Publicly Available Personal Data Compliantly*, GRC SOLUTIONS (Sept. 18, 2023), <https://www.dqmgrc.com/blog/data-scraping-how-to-use-publicly-available-personal-data-compliantly> [<https://perma.cc/NDS8-NGNS>].

In the European context, the episode underscores both the strengths and limits of GDPR enforcement. The GDPR's expansive territorial reach can convert localized biometric scraping into global legal exposure, yet enforcement asymmetries reveal how even robust privacy regimes struggle to control AI-driven re-identification conducted extraterritorially.

Together, the United States and EU approaches reflect two complementary failures: punishment without prevention versus prohibition without execution.

III. THE SELF-REGULATORY SOLUTION

The preceding case studies reveal a common structural failure across biometric-AI governance models. Centralized *ex ante* regulation can promote design-stage safeguards, but struggles with extraterritorial enforcement. Litigation-driven oversight can deter misconduct, but does so unevenly and often too late. Settlement-based enforcement can inadvertently legitimize invasive practices. Together, these cases demonstrate that neither public regulation nor private litigation alone can reliably align innovation incentives and biometric accountability at scale. This section therefore turns to institutional solutions that operate upstream of harm, supplement formal regulation, and provide durable governance capacity across jurisdictions.

As introduced earlier, a self-regulatory organization (SRO) provides a hybrid governance model that combines industry expertise with public oversight. A biometric-AI SRO could establish tiered certification frameworks for biometric systems before deployment, require standardized technical and governance disclosures, and develop performance benchmarks that address accuracy, bias, model drift, and system robustness. It could provide shared compliance infrastructure such as template policies for consent, retention, notice, and security, thereby reducing legal uncertainty across regulatory environments. Continuous monitoring and incident-reporting mechanisms could enable earlier detection of risk, while disciplinary tools—including suspension or public delisting—would reinforce transparency and accountability. Through structured cooperation with public regulators, an SRO could align oversight strategies while incorporating proportionality mechanisms and safe harbors that reduce over-deterrence without undermining substantive

accountability. Created through industry collaboration and formally authorized by public regulators—including the EU AI Office and the FTC—the organization would operate as a co-regulatory institution that combines private technical expertise with public oversight.

A. *The European Union SRO*

Although the European Union already operates one of the most comprehensive and precautionary biometric-AI governance regimes in the world, its multilayered structure generates significant operational, technical, and institutional frictions. Within this context, the introduction of a biometric-AI SRO would be difficult to implement, but highly beneficial.

An SRO would not displace the AI Act or GDPR, nor would it weaken the EU's commitment to fundamental rights. Instead, it would complement the EU's *ex ante* framework by providing flexibility, technical standardization, and rapid interpretive clarity—capacities that EU institutions currently cannot deliver at scale. In doing so, an SRO would directly address the governance gaps of the EU framework identified in Section II, strengthening enforcement capacity while reducing unnecessary barriers to lawful innovation.

One of the most pressing gaps concerns the operation of *ex ante* conformity assessments. As discussed in Section II, these assessments are costly, slow, and uneven across EU Member States due to variations in the expertise of notified bodies and the capacity of market surveillance authorities. An SRO could streamline this process by issuing unified technical standards, best-practice documentation, and pre-assessment protocols that providers could rely upon before formal review. Acting as a centralized interpretive hub, the SRO would reduce divergent national understandings of core concepts such as “high risk” or “systemic risk,” lower duplicative compliance burdens, and make the EU AI Act's preventative ambitions more administrable in practice.

These benefits would be particularly pronounced for small and medium-sized enterprises. SMEs face disproportionate compliance costs, which can lead to existential deployment delays and persistent uncertainty due to limited legal and technical

resources. An SRO could mitigate these barriers by offering shared testing environments, pooled audit resources, open-source compliance tools, and model-evaluation sandboxes, thereby reducing barriers to entry. By stabilizing compliance expectations, the SRO would be analogous to existing organizations such as FINRA or the NYSE within their individually highly technical domains. This would serve as a cost-reducing intermediary, allowing smaller actors to innovate without the risk of inadvertent noncompliance or post-deployment enforcement shocks.

An SRO would also help resolve a structural mismatch between static statutory risk classifications and rapidly evolving biometric technologies. The EU AI Act's Annex III high-risk list, while conceptually sound, is slow to update and vulnerable to strategic reclassification by providers. Through rapid-cycle technical standards and dynamic risk taxonomies, an SRO could respond to emerging biometric uses, such as emotion analysis, behavioral biometrics, and multimodal identification, far more quickly than legislative revision allows. In doing so, it could also serve as an early-warning system for the AI Office, signaling when new practices warrant regulatory attention and preventing enforcement blind spots from developing.

Beyond internal governance challenges, an SRO could strengthen the EU's extraterritorial reach in ways that formal enforcement alone cannot. As the *Clearview* case demonstrates, even deletion orders and substantial fines lose deterrent force when applied to actors without a meaningful EU presence. An industry-backed certification regime administered by an SRO could function as a *de facto* market-access requirement. European companies, cloud providers, and public procurers could require SRO compliance as a contractual condition, compelling foreign vendors to adhere to EU-aligned biometric standards, even where DPAs lack effective enforcement leverage. This form of private-sector leverage would complement existing public enforcement mechanisms rather than relying solely on the GDPR's Article 3 enforcement limitations.

At the same time, an SRO could alleviate the chronic technical capacity constraints facing DPAs and MSAs. No single authority can maintain sustained expertise across high-volume, high-speed biometric AI systems. An SRO could function as a centralized technical brain, developing uniform performance benchmarks for

accuracy, demographic bias, and model drift, as well as standardized evaluation protocols. By issuing binding or semi-binding codes of conduct for participating firms, the SRO would reduce interpretive fragmentation and enforcement burdens while preserving public authorities' ultimate supervisory role.

Finally, an SRO could reduce the procedural friction created by overlapping EU digital legislation and multilevel oversight. Developers currently face a complex web of obligations under the EU AI Act, GDPR, DSA/DMA, and Data Act, all of which are administered by multiple authorities with distinct mandates. An SRO could harmonize compliance expectations by producing consolidated technical guidance that maps how these regimes interact in practice. Serving as a single source of technical truth, the SRO would reduce reliance on slow, formal guidance processes and provide clearer pathways for lawful biometric AI development.

Importantly, such an organization would not undermine the EU's existing regulatory architecture. A biometric-AI SRO would fit within and materially enhance the existing processes. Operating under soft oversight by the EU AI Office, an SRO would improve the administrability of the EU AI Act rather than dilute it, allowing the EU to preserve strong rights-based protections, while mitigating the opportunity costs associated with heavy *ex ante* regulation. By shifting some compliance from rigid statutory interpretation to flexible technical norms, the SRO would reduce over-deterrence, accelerate pre-market review, and help ensure that precautionary regulation does not inadvertently stifle beneficial biometric innovation.

At the same time, the limits of an SRO must be acknowledged. Extraterritorial enforcement—particularly deletion orders against foreign actors—ultimately remains a function of state authority; an SRO can supplement but not replace public enforcement power. Its guidance may also be contested where MSAs assert divergent legal interpretations, especially in politically sensitive biometric contexts. Additionally, the creation of a new regulatory body entails costs. It also raises familiar concerns about institutional complexity and the risk of regulatory capture, particularly where regulators and industry operate in close proximity.

On balance, however, the case for an EU biometric-AI SRO is compelling. Despite foreseeable implementation challenges—including political fragmentation, Member State sovereignty, and

institutional inertia—the EU stands to benefit significantly from an organization that fills the operational gaps of its *ex ante* system. An SRO would improve regulatory speed, consistency, and technical competence without weakening rights protections. By reducing administrative strain and interpretive fragmentation, it would help ensure that the EU’s ambitious regulatory framework is not undermined by slow updates or uneven enforcement. The result would be a more adaptable, innovation-supportive governance regime that remains firmly anchored in precaution and fundamental rights.

B. The United States SRO

A biometric-AI SRO would generate the greatest marginal benefit in the United States. Unlike the EU, which already operates a comprehensive, albeit slow and rigid, regulatory architecture, the United States suffers from a regulatory vacuum into which an SRO can immediately bring coherence, uniformity, and predictable innovation incentives.

The SRO model maps naturally onto longstanding US governance traditions. When technological domains become too complex for direct federal oversight (*i.e.*, securities trading, derivatives markets, domain name systems), Congress has historically delegated regulatory authority to expert SROs operating under federal supervision. Given the rapid development, technical complexity, and systemic risks of biometric AI, traditional notice-and-comment rulemaking cannot easily keep pace with innovation. As a result, an SRO would not represent a radical institutional departure, but rather a familiar and legitimate extension of US administrative practice.

One of the most significant deficiencies an SRO could address is the US system’s reliance on *ex post* enforcement. As demonstrated in Section II through cases involving Meta, Amazon, and Clearview, regulatory rules are often learned only after harm has already occurred, whether through litigation or FTC action. This lag creates prolonged periods during which risky biometric systems operate without meaningful oversight. An SRO could replace this reactive posture with pre-deployment obligations—including audit protocols, standardized documentation, training data disclosures, and consent architecture checks. Continuous monitoring and incident-reporting requirements would further

enable earlier detection of misuse, shifting governance from a “wait for lawsuits” model to proactive risk management.

Fragmentation across state laws presents a second structural failure point. Divergent regimes, such as Illinois’ BIPA, Texas’ CUBI, and jurisdictions with no biometric statutes at all, create a patchwork that is unpredictable, litigation-heavy, and fundamentally incompatible with national AI development. An SRO could mitigate this fragmentation by issuing uniform national technical and procedural standards that firms voluntarily adopt but which, through network effects, become industry baseline norms. By harmonizing expectations for consent, retention, data minimization, accuracy, and auditability, the SRO could function as a *de facto* one-stop shop in a system where federal preemption remains politically elusive.

Excessive reliance on private litigation also generates over-deterrence, especially for small and mid-sized firms. As demonstrated in Section II, statutory damages regimes often penalize technical noncompliance as harshly as substantive harm, exposing firms to existential liability for procedural lapses, including, for example, a missed retention schedule, even where no consumer injury is alleged. An SRO could introduce proportionality into enforcement through tiered compliance obligations, safe harbors, and cure periods that distinguish minor deficiencies from genuinely harmful practices. This model would preserve accountability while offering SMEs more straightforward rules and lower-risk operating conditions, thereby supporting competition and innovation.

Institutional capacity further weakens US governance. Although the FTC’s Section 5 authority is broad, it is simultaneously shallow: the FTC lacks the staff, specialized expertise, and statutory tools for systematic pre-market review of biometric-AI systems. An SRO could fill this gap by serving as the industry’s technical nucleus, centralizing expertise on accuracy metrics, demographic bias, data lineage, model drift detection, and adversarial testing. In a delegated oversight model, mirroring how the SEC relies on FINRA’s technical surveillance with respect to brokers, the FTC could leverage SRO evaluations to focus enforcement on serious violations, rather than attempting to build in-house technical capacity from scratch.

Litigation-driven governance also fails to produce stable, forward-looking rules. Case law yields sporadic and conflicting interpretations of key concepts, such as “biometric identifiers,” “collection,” and permissible iterative training practices.³⁹⁶ The SRO could issue continuously updated, technology-specific standards that clarify these ambiguities before disputes arise. By publishing public rulebooks, the SRO would do what courts cannot: set stable expectations *ex ante*, thereby reducing regulatory arbitrage, forum shopping, and judicial inconsistency.

Scalability presents another challenge. Biometric-AI systems are proliferating across retail, employment, healthcare, and law enforcement—overwhelming the combined enforcement capacity of the FTC, state attorneys general, and private litigants. An SRO could conduct routine monitoring, certification, and compliance checks on a scale that government agencies cannot. Centralized audit logs, incident reporting systems, and a public registry of certified systems would enhance visibility across an otherwise opaque industry, enabling regulators to target high-risk actors more effectively.

Finally, an SRO could correct the distorted incentives created by procedurally weak settlements, as portrayed in Clearview’s equity agreement. Litigation outcomes that preserve core business models while imposing nominal or misaligned penalties undermine deterrence and normalize invasive practices. An SRO could impose independent disciplinary measures such as suspension or revocation of its specific certification, directly affecting a firm’s ability to operate. These consequences would be behavior-changing, rather than financially engineered, ensuring that compliance cannot be purchased through creative settlements alone.

A US biometric-AI SRO would not replace federal oversight, but would operationalize it. Federal law would define the regulatory floor, while the SRO would build the technical infrastructure necessary for compliance. Agencies could rely on the SRO’s monitoring, reporting, and certification to concentrate enforcement resources on the most serious violators. The resulting

396. *Cf.* *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186; *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019); *Rivera v. Google Inc.*, 366 F. Supp. 3d 998 (N.D. Ill. 2019); *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004.

system would be faster, more expert-driven, and administratively scalable—qualities that are currently impossible under existing US conditions.

As in the EU, the limits of a US SRO model must be acknowledged. Federal legislation would still be required to authorize SRO authority, preempt inconsistent state laws, and ground enforcement in democratic legitimacy. Certain public sector uses, such as federal law enforcement deployments, would require statutory rules beyond private governance. While the SRO cannot entirely eliminate the possibility of litigation, it can significantly shape its scope and reduce uncertainty.

In conclusion, the United States is the jurisdiction where biometric-AI SRO governance is not only helpful, but ultimately essential. Given federal inertia, state-level fragmentation, and rapid technological evolution, an SRO would offer the first coherent national governance system. By replacing reactive enforcement with proactive oversight, injecting technical expertise into the regulatory ecosystem, and reducing over-deterrence through proportionality and clarity, a biometric-AI SRO would provide the structural foundation that the United States currently lacks—benefiting innovators, regulators, and consumers alike.

C. *The Pros and Cons of the Self-Regulatory Model*

Although the European Union and the United States approach biometric-AI governance from distinct legal and normative traditions, technology does not respect jurisdictional boundaries. Biometric AI models are trained on globally sourced data, operate through multinational cloud infrastructure, and are deployed simultaneously across markets. As a result, purely domestic regulatory solutions, whether the EU's rights-centric *ex ante* regime or the United States' litigation-driven *ex post* system, inevitably leave gaps. The EU's core challenge lies in regulatory complexity and institutional slowness, while the United States faces fragmentation and the absence of comprehensive federal rules. A harmonized SRO architecture, as portrayed by the current governing systems of financial markets and cybersecurity, allows each jurisdiction to retain its governance identity while converging on shared technical standards, risk controls, and oversight mechanisms. The result is a dual-SRO system, one operating within the EU's statutory framework and one operating under US federal

delegation, that cooperates through a common technical core, enabling global interoperability without the need for legal harmonization. In effect, it separates legal philosophy from technical governance, allowing cooperation where alignment is feasible and divergence where it is unavoidable.

Harmonization is necessary because biometric AI is inherently transnational in nature. Without coordination, firms must navigate two incompatible regulatory styles, resulting in inconsistent risk controls and fragmented market access. Existing enforcement asymmetries already demonstrate the risk of regulatory arbitrage. Companies can route operations through jurisdictions with weaker or slower enforcement. Clearview illustrates how US leniency undermines EU protections, while the EU's procedural rigidity incentivizes companies to pre-launch primarily in the United States. A harmonized SRO reduces arbitrage by establishing convergent technical requirements, regardless of geography.

Structurally, the model would rely on two cooperating SROs supported by shared standards. Joint transatlantic committees would define baseline global risk metrics, such as accuracy, demographic error rates, model drift indicators, and adversarial robustness. These committees would also publish unified documentation requirements, including model cards, data lineage disclosures, and training protocols, while maintaining a common taxonomy of biometric systems spanning facial recognition, gait, voice, behavioral, and multimodal identification. Interoperability standards for audit logs, redress mechanisms, and transparency reporting would further ensure that systems evaluated in one jurisdiction can be meaningfully assessed in the other.

Certification would form the backbone of this harmonized structure. Each SRO would issue certifications that are mutually recognized across the Atlantic; for example, a certification could indicate conformity with the EU's high-risk requirements, compliance with a US federal safe harbor, or joint EU-US market readiness. Over time, such certifications would function as a global market passport, akin to ISO standards. This approach preserves regulatory sovereignty while creating powerful market incentives for compliance.

A shared incident reporting and cross-border alert mechanism would further enhance global oversight and

coordination. Either SRO could flag emergent biometric vulnerabilities or general noncompliant practices. These alerts would operate similarly to information-sharing arrangements in financial regulation, enabling faster responses to systemic risks even when formal statutory enforcement is slow or jurisdictionally constrained.

The advantages of a harmonized SRO model are substantial. For developers, it would replace duplicative and conflicting compliance pipelines with a single technical baseline, reducing engineering, legal, and operational costs while creating predictable incentives. For regulators, pooled technical expertise would strengthen oversight in areas where no single authority currently has sufficient capacity, reducing the risk of “bias shopping” or uneven performance across populations. Enforcement capacity would also improve, as EU DPAs and US agencies could rely on SRO audit logs and certifications to target serious violations more efficiently, including by threatening certification withdrawal as a market-access consequence.

Perhaps, most importantly, harmonization would significantly reduce regulatory arbitrage. Firms would no longer be able to treat the United States as a permissive testing ground or the EU as a procedurally slow but ultimately avoidable constraint. A common compliance floor across markets would stabilize incentives around privacy-preserving design, secure data architecture, and accountable model development.

That said, harmonization has limits. Fundamental rights frameworks cannot be fully aligned, and the EU’s rights-based model cannot be collapsed into the United States’ harm-based approach. Differences in law enforcement authority and public sector uses of biometric AI will persist, and without a federal privacy statute, the US SRO’s authority would remain narrower than its EU counterpart. Some actors may also remain outside the certification ecosystem until commercial pressure forces them to participate.

More broadly, SROs are not costless. They require institutional infrastructure, staffing, and sustained funding—typically financed through industry fees rather than public taxation. This funding model raises familiar concerns about regulatory capture and proximity between regulators and industry. Yet these concerns are neither unique nor decisive.

Similar dynamics exist throughout public administration, and decades of experience with financial and technical SROs demonstrate that capture risks can be mitigated through transparency, public oversight, and balanced governance structures.

The cost-benefit calculus differs slightly between the EU and the United States. In Europe, where a dense regulatory architecture already exists, the marginal cost of an SRO would be relatively small compared to the benefits of improved coordination, technical consistency, and reduced fragmentation. In the United States, where no comprehensive framework exists, the justification is even more substantial. Bearing the cost of an SRO is worthwhile precisely because it injects expertise, coherence, and forward-looking governance into a system otherwise defined by federal inertia and state-level patchwork.

Taken together, a harmonized transatlantic SRO architecture presents a realistic yet optimistic path toward global biometric-AI governance. It preserves jurisdictional autonomy while enabling technical convergence, reduces arbitrage without legal harmonization, and aligns innovation incentives with accountability. In a domain defined by speed, scale, and cross-border data flows, such a structure is not merely desirable—it is increasingly necessary.

IV. CONCLUSION

Biometric AI exposes structural weaknesses in both the European Union's precautionary regulatory regime and the United States' litigation-driven approach. While each system offers important safeguards, neither alone provides the adaptive, technically informed governance necessary to manage rapidly evolving biometric technologies at scale, particularly those integrated with artificial intelligence. The EU's *ex ante* model promotes strong rights-based protections but struggles with speed, uniformity, and extraterritorial enforcement. The US system, by contrast, enables flexibility and innovation but relies too heavily on reactive, fragmented enforcement that often occurs only after harm has materialized. As biometric systems become more pervasive, data-intensive, and globally deployed, these limitations become increasingly consequential.

This Note has argued that a harmonized self-regulatory organization (SRO) model offers a viable institutional solution to these challenges. By embedding technical expertise within a structural framework of industry coordination and public oversight, an SRO could establish consistent standards for data governance, model performance, and accountability while adapting more rapidly than traditional legislative or judicial mechanisms. In the EU, such an organization would complement the EU AI Act by improving administrability, reducing fragmentation, and enhancing technical capacity. In the United States, it would provide long-needed coherence, replacing reactive enforcement with proactive oversight and mitigating the inefficiencies of state-level divergence. Through certification systems, shared compliance infrastructure, and continuous monitoring, SROs could align incentives across actors while preserving both innovation and fundamental protections.

At a transnational level, a dual-SRO architecture would enable convergence around shared technical standards without requiring full legal harmonization. By coordinating risk metrics, audit protocols, and transparency requirements, cooperating SROs could reduce regulatory arbitrage, streamline compliance, and strengthen global accountability for biometric AI systems. While such a model is not without risks, concerns about regulatory capture, institutional complexity, and the limits of private enforcement are all challenges manageable within a framework of public supervision and transparency. Ultimately, as biometric AI continues to evolve across borders and sectors, governance models must evolve accordingly. A harmonized SRO framework represents a realistic and necessary step toward a more adaptive, interoperable, and effective system of biometric AI governance.