Essays

Regulatory Tipping Point: Key Lessons from a Divergence in AI Regulation Between the EU and the US

Jordan L. Fischer*

ABSTRACT: In the last five years, artificial intelligence technologies have exploded onto the global stage. At the same time, different regions have drastically diverged in the approach to regulating artificial intelligence. This article explores two dominate players in the artificial intelligence world: the European Union and the United States, and discusses, in turn, how each has approached regulating artificial intelligence and lessons learned for the next wave of artificial intelligence development and regulation.

KEYWORDS: artificial intelligence; United States regulation; European regulation; comparative analysis; emerging technologies

1. Introduction

In the last five years, the use of artificial intelligence exploded across the globe, impacting individuals in their daily lives, businesses in their day-to-day operations, and dominating discussions at all levels. For the most part, this technology remained, and continues to remain, unchecked, with major players innovating without guardrails or regulatory requirements.

Within this backdrop, the European Union (EU) adopted the EU Artificial Intelligence Act (the EU AI Act), the first attempt to create a comprehensive regulatory framework around the use of artificial intelligence. However, unlike the EU's adoption of the General Data Protection Regulation in 2018, which became a dominant global force with many countries adopting a similar law in their country, widescale adoption of the EU AI Act has not been embraced, and there is even push back on the EU AI Act within the EU and beyond. On the contrary, many countries are intentionally pausing artificial

* *Drexel University, Thomas R. Kline School of Law. Mail: jlf324@drexel.edu.* *This article was subject to a blind peer review process.*

intelligence regulation, or, as in the United States, intentionally restricting the creation of artificial intelligence laws and regulations.

This article lays out that artificial intelligence regulation is at a unique tipping point: will countries follow a more European model and adopt some regulatory guardrails around the creation and use of artificial intelligence? Or will countries instead allow artificial intelligence to develop unchecked, putting innovation and economic concerns above any potential negative impacts of the rapid adoption of artificial intelligence?

Part I explores the two different, and dominant, regulatory approaches to artificial intelligence: first, the more regulatory heavy focus in the EU and second, the more hands-off approach to artificial intelligence regulation in the U.S. To date, the EU has taken a proactive regulatory approach to the creation and adoption of artificial intelligence. Conversely, the U.S. appears to be focusing solely on innovation and encouraging the development of artificial intelligence, with little to no regulatory guardrails. Part II looks at the comparison of the EU and the U.S. Part III will discuss lessons learned to date, and ways to consider a path forward in regulating artificial intelligence on the global stage.

2. Overview of the EU and the U.S. Approaches to Artificial Intelligence Regulation

It should come as no surprise that the EU and the U.S. take different approaches to regulation, and are diverging dramatically in the context of artificial intelligence.[1] Historically, in Europe, both at the EU level as well as at the Member State level, governments have favored adopting regulation across a wide sector of industries and areas of society. The EU, in some ways, takes a more paternalistic approach, protecting individuals against corporations and the government alike. This is best exemplified by recent regulatory approaches to technology within the EU, creating comprehensive and protective regulations that focus on the individual rights, and protection from corporate actors.[2]

Contrast the EU approach with the U.S., where the focus is more market driven, with data, and subsequently privacy, made into more of a commercial asset as opposed to a regulated right. The U.S. approach to the digital economy is often an "uncompromised faith in markets and skepticism toward government regulation".[3] The U.S. comes from a more techno-libertarian ethos, an approach that emphasizes individual freedom, minimizes government intervention, and focuses on the potential for technology to create a "free" (meaning no regulation, not no cost) and unregulated online environment.

This dichotomy in the approaches between the EU and the U.S. is no more relevant than in the context of the technology industry. There is this widely accepted view in the U.S. that regulation will hamper innovation, a view that is heavily promoted by technology companies themselves. Instead, the U.S. has placed a large reliance on the market and self-regulation to keep technology companies in check. As Anu Bradford sums up, "most governments have refrained from regulating the tech industry precisely

[1] A. ENGLER, *The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment*, in *Brookings Institution*, 2023, available at https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/ (last visited 30/09/2025).

[2] NEWMAN, L. ABRAHAM, *Protectors of Privacy*, in *Cornell University Press*, 2008 (describing the European comprehensive approach to privacy regulation).

[3] A. BRADFORD, *The False Choice Between Digital Regulation and Innovation*, in *Nw.U.L.Rev*, 119, 2024, 377-387.

because of their fear that attempts to interfere with tech companies' operations would undermine their innovative capacity".[4]

This article will explore these divergent approaches to technology regulation (or lack of regulation) in the context of artificial intelligence. The EU, aligning with its historical approach, has taken a regulation first approach to artificial intelligence with its adoption of the EU AI Act. The U.S., conversely, has been slow to adopt regulation for artificial intelligence in the federal context, even briefly considering (and the ultimately rejecting) a formal federal moratorium on artificial regulation for a period of ten years. The lack of federal legislation on artificial intelligence has given way to a state-by-state patch work approach to artificial intelligence regulation. We will explore each in turn.

2.1. The European Proactive Approach in Adopting the EU AI Act

The EU AI Act is touted as the "first regulation on artificial intelligence".[5] The European Commission initially proposed the original draft of the EU AI Act in 2021, incredibly early in the adoption of artificial intelligence technologies across the globe.

It is interesting to place the adoption of the EU AI Act in the context of the artificial intelligence commercial marketplace. ChatGPT first became available to the general public as a free research preview on November 22, 2022.[6] Within two months of its initial release, ChatGPT was estimated to have reached 100 million users, far surpassing the adoption rate for other technologies like Facebook, Instagram, and TikTok.[7] In one year, the number of users grew to more than 100 million, and in two years, that number grew to 350 million users.[8] It is estimated that approximately 10% of the global adult population is using ChatGPT by mid-2025.[9]

The EU AI Act was ahead of the curve, introduced a year before ChatGPT became available to the mass market. While artificial intelligence was already used in certain commercial products,[10] its mass adoption rates coincided with the same timeline for final adoption of the EU AI Act, which was fully adopted in June 2024.

The EU AI Act lays out a set of risk-based rules for the creation and use of artificial intelligence in Europe. It is part of the EU's larger digital strategy to create a comprehensive regulatory approach

[4] BRADFORD, *op. cit.*, 379.

[5] European Parliament, *EU AI Act: first regulation on artificial intelligence*, February 19, 2025, available at https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (last visited 30/09/2025).

[6] *History Of ChatGPT: A Timeline Of The Meteoric Rise Of Generative AI Chatbots*, in *Search Engine Journal*, 2024, available at https://www.searchenginejournal.com/history-of-chatgpt-timeline/488370/ (last visited 30/09/2025).

[7] *ChatGPT sets record for fastest-growing user base - analyst note*, in *Reuters*, 2023, available at https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/ (last visited 30/09/2025).

[8] A. CHATTERJI *et al, How People Use Chatgpt*, in *NBER*, Working Paper No. 34255, 2025, available at http://www.nber.org/papers/w34255 (last visited 30/09/2025).

[9] *Ivi,* 10.

[10] *What is the history of artificial intelligence (AI)?,* in *Tableau*, available at https://www.tableau.com/data-insights/ai/history (last visited 30/09/2025).

across Europe for a variety of digital areas.[11] This strategy includes the Digital Services Act (DSA),[12] the Digital Markets Act (DMA),[13] and the Data Governance Act (DGA),[14] in addition to the EU AI Act. The EU's General Data Protection Regulation (GDPR),[15] adopted in 2018, was the first regulation in the EU's concerted effort to develop controls around the use of technology, and the outsized role that large technology companies play in everyday society.

Each of these laws are intended to focus on different aspects of the digital space. The DSA attempts to create a safer and fairer digital space by regulating online intermediaries (platforms, marketplaces, social networks, etc.) and enhancing accountability. The DMA focuses on competition in the digital space, and specifically anti-competitive practices by larger technology companies. And, the DGA attempts to create a framework for the sharing and reuse of data, particularly public sector data, while addressing data protection and ethical considerations. The GDPR focuses on the use of personal information across any platform or use case, whether it includes technology or not.

The EU AI Act builds on these other regulations with a specific focus on artificial intelligence technologies. Specifically, the EU AI Act lays out expectations for providers and deployers of "AI systems"[16] to limit the risks of artificial intelligence, especially high-risk use-cases. A provider is defined as 'a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge'.[17] A deployer is defined as "a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity".[18]

---

[11] European Commission Digital Strategy, 2022, available at https://commission.europa.eu/publications/european-commission-digital-strategy_en (last visited 30/09/2025).

[12] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (*Digital Services Act*), available at http://data.europa.eu/eli/reg/2022/2065/oj.

[13] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (*Digital Markets Act*), available at http://data.europa.eu/eli/reg/2022/1925/oj.

[14] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (*Data Governance Act*), available at http://data.europa.eu/eli/reg/2022/868/oj.

[15] 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*), available at http://data.europa.eu/eli/reg/2016/679/2016-05-04.

[16] An "AI system" is defined as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." EU *AI Act*, Article 3(1).

[17] EU *AI Act*, Article 3(3).

[18] EU *AI Act*, Article 3(4).

There are four risk levels under the EU AI Act: unacceptable risk, high risk, limited risk, and minimal risk.[19] The EU AI Act provides guidance in determining where a given AI tool or use-case may sit within these risk levels, and then provides corresponding requirements based on the risk-level identified.

The ultimate goal of the EU AI Act is two-fold: first, to create "trustworthy AI"; and second, to create governance around the development and deployment of artificial intelligence within the EU. Specifically, the EU AI Act is intended "to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation".[20]

In many ways, the EU attempted to right a perceived error on their part with the early adoption of the EU AI Act to try to halt the unrestrained development and then mass use of artificial intelligence, as opposed to retroactively apply regulatory controls, as it did with personal information under the GDPR. The GDPR, from a very practical sense, was arguably too late to really restrain the massive data collection, and use, of personal information by private companies, making it challenging to actually enforce privacy protections with these companies that survive on massive data ingestion. Learning from that experience, the EU is attempting to set the guidelines for AI before it becomes a dominate force in society, and almost an inevitable technology we all must live with.

However, the EU AI Act faces numerous hurdles to its enforcement. On the eve of its effective date, numerous stakeholders continue to push for it to be delayed and/or amended before it goes into full effect. For example, in an open letter, forty-five (45) of Europe's largest companies called on the European Commission to pause the EU AI Act's most stringent requirements for two years.[21] Criticism of the EU Act has taken various forms, including a lack of certainty and guidance from the EU on how the EU AI Act will be enforced, the cost of compliance creating huge hurdles for businesses, especially small to medium sized businesses, and the lack of clear standards for businesses to use to create effective compliance to comply with the EU AI Act. The ultimate success of the EU AI Act in creating effective controls on artificial intelligence will play out over the coming years.

2.2. The U.S. Disjointed Approach to AI Regulation

Artificial intelligence is facing a similar path as most technology regulation in the U.S.: a divide between the federal and the state governments. Similar to data protection regulation, which has seen more movement in at the state level than the federal level, the U.S. states have taken a more proactive stance on artificial intelligence regulation as compared to the federal level. However, the federal government has not remained silent on artificial intelligence, providing guidance in other forms outside of traditional regulation.

---

[19] *High-level summary of the AI Act*, in *EU AI Act*, 2024, *available at* https://artificialintelligenceact.eu/high-level-summary/ (last visited 30/09/2025).

[20] *EU AI Act*, Preamble.

[21] *EU AI Champions Open Letter Stop-the-clock to reset the EU's AI ambitions*, July 3, 2025, available at https://docs.google.com/document/d/16570SgWppeeeYINe4WydTbG2ioBTPdOW_fmfMbmg6sY/edit?pli=1&tab=t.nwpblityhtt3.

2.2.1. The U.S. Federal Artificial Intelligence Initiatives

At the federal level, the U.S. government approach to artificial intelligence has evolved under the two most recent presidential administrations. While the Biden administration focused on creating certain guardrails to the development and use of artificial intelligence, the most recent Trump administration is promoting innovation of artificial intelligence technologies over the development of any artificial intelligence guardrails or regulatory controls. This is best exemplified by the Executive Order 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence"[22] adopted by President Donald J. Trump in his second administration.[23]

Executive Order 14179 "revokes certain existing AI policies and directives that act as barriers to American AI innovation, clearing a path for the United States to act decisively to retain global leadership in artificial intelligence". A key focus of the executive order is "America's global AI dominance"[24] and the promotion of artificial intelligence as a tool for national security and economic competitiveness. By adopting this executive order, the Trump Administration nullified the guardrails and protections included within the President Joseph R. Biden's Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence".[25] Executive Order 14110 had established eight guiding principles for the development and use of artificial intelligence technologies, including that artificial intelligence be safe and secure, innovation be responsible, and that artificial intelligence protect Americans' privacy and civil liberties.[26]

Under the Trump administration, Executive Order 14179 directed the creation of an "Artificial Intelligence Action Plan". In July 2025, the "Winning the Race, AMERICA'S AI ACTION PLAN" was released.[27] The Plan lays out three pillars: (1) Accelerate AI Innovation; (2) Build American AI Infrastructure; and (3) Lead in International AI Diplomacy and Security.

Regarding regulation, the Plan states "[t]he United States needs to innovate faster and more comprehensively than our competitors in the development and distribution of new AI technology across every field, and dismantle unnecessary regulatory barriers that hinder the private sector in doing so".[28] The Plan continues that "AI is far too important to smother in bureaucracy at this early stage, whether

---

[22] *Removing Barriers To American Leadership In Artificial Intelligence*, Executive Order 14179, Jan. 23, 2025, available at https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

[23] It is important to note that E.O. 14179 was not President Trump's first executive order related to AI. In his first term, President Trump adopted Executive Order 13859, *Maintaining American Leadership in AI*, available at https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence. This executive order also focused on the importance of remaining a dominant player in the development of AI technologies for both economic and national security reasons.

[24] *Ibid.*

[25] *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, Executive Order 14110, Oct. 30, 2023, available at https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[26] *Ibid.*

[27] *Winning the Race America's AI action plan*, July 2025, available at https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (last visited 30/09/2025).

[28] *Ivi,* 1.

at the state or Federal level".[29] Specifically addressing any state-level regulation, the Plan explains: "The Federal government should not allow AI-related Federal funding to be directed toward states with burdensome AI regulations that waste these funds, but should also not interfere with states' rights to pass prudent laws that are not unduly restrictive to innovation".[30]

The Trump administration's innovation-first approach to artificial intelligence is further buttressed by the recently adopted "One, Big Beautiful Bill", introduced in May 2025.[31] During its drafting, this bill included a moratorium on artificial intelligence regulation at the state-level or by any political division. Specifically, the Act stated that 'no State or political subdivision thereof may enforce, during the 10-year period beginning on the date of the enactment of this Act, any law or regulation of that State or a political subdivision thereof limiting, restricting, or otherwise regulating artificial intelligence models, artificial intelligence systems, or automated decision systems entered into interstate commerce'.[32]

Ultimately, this moratorium was removed from the final bill before it was passed.[33] However, it echoes the theme of the AI Action Plan: the Trump administration is focused on artificial intelligence innovation and not creating regulation at either the federal or state level.

The U.S. Federal government's lack of AI regulation on the development and deployment of AI needs to be contrasted with a more proactive regulatory approach to the development of certain artificial hardware and the economic tariffs being set by the Trump administration. These can be seen as regulating artificial intelligence, but in a more protectionist approach versus the creation of trustworthy artificial intelligence as seen in the EU.

Under both the Biden and the Trump Administrations, the U.S. has restricted the sale of semiconductor and chip technologies to certain countries. Using export control measures, the Biden Administration first implemented sweeping export control restrictions in 2022 for the sale of advanced U.S. semiconductors and technologies to China. These controls were further enhanced in 2023 with additional restrictions on the sale of these technologies to China.[34] The Trump administration has continued these restrictions under his second administration, and even explored the requirement that for any chips made for non-U.S. users, there must be a chip made for a U.S. use.[35] These semiconductor technologies are key for the development of large scale artificial intelligence modeling that can compete on the global stage.[36]

---

[29] *Ivi,* 3.

[30] *Ibid.*

[31] *H.R.1 – One Big Beautiful Bill Act*, available at https://www.congress.gov/bill/119th-congress/house-bill/1/text.

[32] Sec. 43201(c) of *H.R.1 – One Big Beautiful Bill Act* reported in House on May 20, 2025.

[33] *State AI Regulation Survived a Federal Ban. What Comes Next?*, in *Carnegie Endowment*, 2025, available at https://carnegieendowment.org/emissary/2025/07/ai-congress-bill-state-ban-what-next.

[34] *Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications*, Bureau of Industry & Security, Office of Congressional and Public Affairs, Dec. 2, 2024, available at https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military (last visited 30/09/2025).

[35] *U.S. plans 1:1 chip production rule to curb overseas reliance*, *WSJ reports*, in *Reuters*, Sep. 26, 2025, available at https://www.reuters.com/world/us/us-plans-mandate-11-ratio-domestically-manufactured-imported-chips-wsj-reports-2025-09-26/ (last visited 30/09/2025).

[36] *The Intersection of AI and Semiconductors*, Microchip U.S.A, available at https://www.microchipusa.com/industry-news/the-intersection-of-ai-and-semiconductors-advancements-implications-and-future-opportunities (last visited Sep 30, 2025).

Building on this approach, in August 2022, the U.S. passed the CHIPS and Science Act,[37] which authorized $280 billion to boost domestic research and manufacturing of semiconductors in the United States. The Act is intended to create a more controlled supply chain around the key technologies needed to promote American dominance in the artificial intelligence industry.

Contrary to the more hands-off regulatory approach for the deployment of artificial intelligence technologies into society, the U.S. has taken a much more proactive approach to regulating the tools needed to develop AI technologies: creating barriers to the sale of certain technologies outside of the U.S. (and specifically, China) and encouraging, through huge financial incentives, maintaining AI research and development within the U.S.. These examples highlight the complex role of regulation of artificial intelligence at the U.S. federal level.

2.2.2. Existing U.S. Federal Regulations That Impact Certain AI Use Cases

The lack of a specific Federal artificial intelligence regulation on the use of artificial intelligence technologies does not mean that there are no regulations that could impact specific use cases of artificial intelligence within the U.S. Existing laws such as the Health Insurance Portability and Accountability Act (HIPAA)[38] and the Federal Trade Commission Act (FTC Act)[39] are being leveraged in certain instances to create protections around the deployment of artificial intelligence.

The U.S. Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), is charged with enforcing HIPAA. In this role, OCR issued a "Dear Colleague" letter in January 2025 related to "Ensuring Nondiscrimination Through the Use of Artificial Intelligence and Other Emerging Technologies".[40] In this January 2025 OCR Letter, OCR clearly calls out the need to balance the value that the healthcare industry can receive from the use of artificial intelligence technologies, with the potential risks to patients for discriminatory treatment. OCR adopted final rule implementing Section 1557 in 2024, which "prohibits discrimination on the basis of race, color, national origin, age, sex, and disability in health programs or activities that receive Federal financial assistance from HHS, health programs or activities established under Title I, such as State-based Exchanges, and HHS-administered health programs or activities, including the Federally-facilitated Exchanges".[41]

The January 2025 OCR Letter clarifies that these anti-discrimination requirements apply equally to any "patient care decision support tool" including those tools that leverage artificial intelligence. In short, OCR is taking the position that the HIPAA regulation, and its corresponding protections, are technology agnostic, and will apply equally to artificial intelligence as well as other technologies.

Turning to the Federal Trade Commission (the FTC), the FTC is, in essence, a consumer protection and antitrust regulator.[42] The FTC Act, Section 5, which is the main governing authority for the FTC, empowers the FTC to investigate and prevent unfair methods of competition, and unfair or deceptive

[37] 136 Stat. 1366, available at https://www.congress.gov/bill/117th-congress/house-bill/4346.
[38] Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[39] 15 U.S.C. § 45.
[40] Department of Health & Human Services, Letter re: *Ensuring Nondiscrimination Through the Use of Artificial Intelligence and Other Emerging Technologies*, January 10, 2025 (hereinafter, "January 2025 OCR Letter").
[41] January 2025 OCR Letter, 1-2.
[42] Federal Trade Commission, *What the FTC Does*, available at https://www.ftc.gov/news-events/media-resources/what-ftc-does (last visited 30/09/2025).

acts or practices affecting commerce.[43] The FTC is leveraging both competition and unfair or deceptive acts in the context of artificial intelligence to protect consumers against any harm created by artificial intelligence technologies.

In January 2025, the FTC provided a detailed overview of its position on artificial intelligence and potential consumer harms that may result from the use of artificial intelligence.[44] In this overview, the FTC makes clear that AI is not exempt from existing laws:

> Because there is no AI exemption from the laws on the books, firms deploying these AI systems and tools have an obligation to abide by existing laws, including the competition and consumer protection statutes that the FTC enforces. FTC staff can analyze whether these tools violate people's privacy or are prone to adversarial inputs or attacks that put personal data at risk. We can also scrutinize generative AI tools that are used for fraud, manipulation, or non-consensual imagery, or that endanger children and others. We can consider the impacts of algorithmic products that make decisions in high-risk contexts such as health, housing, employment, or finance. Those are just a few examples, but the canvas is large.[45]

This is a strong statement reminding all developers and deployers of AI that they are subject to regulatory oversight, even if no stand-alone AI law currently exists.

The FTC further lays out a number of factors that businesses should take into account when leveraging AI in their operations, including:

1. Taking necessary steps to prevent harm before and after deploying a product.
2. Taking preventative measures to detect, deter, and halt AI-related impersonation, fraud, child sexual abuse material, and non-consensual intimate imagery.
3. Avoiding deceptive claims about AI tools that result in people losing money or put users at risk of harm.
4. Ensuring privacy and security by default.[46]

In February 2024, former Chair and Commissioner, Lina M. Khan, provided remarks on the intersection of competition law and artificial intelligence technologies.[47] In her remarks, Ms. Khan emphasized the need for the FTC to establish "rules of the road for AI".[48] She laid out four areas where the FTC is focusing on artificial intelligence technologies from a competition lens. First, the FTC is reviewing any existing or emerging bottlenecks across the AI stack. History shows that firms that capture control over key inputs or distribution channels can use their power to exploit those bottlenecks, extort customers, and maintain their monopolies".[49] Second, the FTC is "focused on how business models drive incentives"

[43] *Ibid.*; *Federal Trade Commission Act* (FTC Act), 15 U.S.C. §§ 41-58, at §45(a)(1).
[44] Federal Trade Commission, *AI and the Risk of Consumer Harm*, January 3, 2025.
[45] *Ibid.*
[46] *Ibid.*
[47] Federal Trade Commission, *A few key principles: An excerpt from Chair Khan's Remarks at the January Tech Summit on AI*, February 8 2024, available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/few-key-principles-excerpt-chair-khans-remarks-january-tech-summit-ai (last visited 30/09/2025).
[48] *Ibid.*
[49] *Ibid.*

and that "[t]he drive to refine your algorithm cannot come at the expense of people's privacy or security, and privileged access to customers' data cannot be used to undermine competition".[50]
Third, the FTC is aiming to align "liability with capability and control. This requires looking upstream and across layers of the AI stack to pinpoint which actor is driving or enabling the lawbreaking".[51] Fourth, the FTC, recognizing the uniqueness created by AI, is looking to create "effective remedies that establish bright-line rules on the development, use, and management of AI inputs".[52] For example, in the FTC's opinion "some data is simply off the table for training models".[53]
Taken together, the FTC's guidance to date demonstrates that at the federal level in the U.S., there is not a complete absence of any regulatory oversight regarding artificial intelligence. The challenge is that the FTC's authority is somewhat limited to a consumer protection or competition lens. And, often, there are business use cases of artificial intelligence that may fall outside of the scope of the FTC's authority to regulate, leaving certain areas exposed to the risk of little federal regulation or oversight.

2.2.3. The NIST AI Risk Management Framework as a Non-Regulatory Response

Beyond regulation, in January 2023, the National Institute of Standards and Technology (NIST),[54] part of the U.S. Department of Commerce, released the Artificial Intelligence Risk Management Framework (AI RMF), "a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems".[55] While the framework is not a regulation, it does represent the most comprehensive attempt at the federal level, to date, to articulate a structured, socio-technical approach to governing artificial intelligence risks.
The AI RMF, as with all NIST guidance, provides guidance that is "intended to be *voluntary*, rights-preserving, non-sector-specific, and use-case agnostic, providing flexibility to organizations of all sizes and in all sectors and throughout society to implement the approaches in the Framework".[56] It creates a risk-based approach, not unlike the EU AI Act, trying to both "minimize anticipated negative impacts of AI systems and identify opportunities to maximize positive impacts".[57] The AI RMF attempts to provide practical guidance for managing a wide spectrum of harms artificial intelligence systems may produce—ranging from bias and discrimination to safety failures and privacy intrusions. The AI RMF is not limited to technical safeguards; it includes organizational governance, accountability, and the embedding of legal and ethical considerations into the lifecycle of AI systems.
Even though the AI RMF is not a regulation, it still could impact the development of artificial intelligence technologies and at least provide a framework to assess the technologies against certain guardrails and controls. As in other areas of emerging technology, voluntary standards often evolve into benchmarks

[50] *Ibid.*
[51] *Ibid.*
[52] *Ibid.*
[53] *Ibid.*
[54] NIST is charged with creating standards in various fields of science and technology.
[55] *Artificial Intelligence Risk Management Framework* (AI RMF 1.0), NIST AI 100-1, January 2023, available at https://doi.org/10.6028/NIST.AI.100-1 (last visited 30/09/2025).
[56] *Ivi*, 2 (emphasis in original).
[57] *Ivi*, 4.

for regulatory expectations, procurement requirements, and even judicial determinations of reasonable care. In the absence of a comprehensive federal artificial intelligence statute, the AI RMF offers a soft law infrastructure that may guide U.S. federal agencies as well as the private sector, helping to provide a foundation for any industry self-regulation or a standard of reasonableness for artificial intelligence.

2.2.4. The U.S. States Attempt to Create Artificial Intelligence Regulatory Initiatives

While artificial intelligence regulation at the federal level in the U.S. remains sparse, the U.S. states continue to push forward with artificial intelligence regulations, either in the form of stand-alone regulations, such as Colorado's AI Act[58] or the Texas Responsible Artificial Intelligence Governance Act,[59] or by leveraging the growing number of comprehensive state-level privacy laws to implement requirements around the use of personal information in automated decision technologies. California is the best example of this second approach. This Article will review each in turn.

Colorado adopted the first comprehensive artificial intelligence regulation in the U.S. in May 2024: An Act Concerning Consumer Protections in Interactions with Artificial Intelligence Systems (the Colorado AI Act). Effective on January 1, 2026, the Colorado AI Act lays out requirements for developers and deployers of artificial intelligence in Colorado.

Drawing parallels to the EU AI Act, the Colorado AI Act defines an "artificial intelligence system" as "any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments".[60] However, the Colorado AI Act focuses exclusively on "high-risk artificial intelligence systems", defined as "any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision".[61]

Breaking down that definition further, the Colorado AI Act defines the terms "substantial factor" and "consequential decision". Substantial factor is "a factor that: (i) assists in making a consequential decision; (ii) is capable of altering the outcome of a consequential decision; and (iii) is generated by an artificial intelligence system".[62] This can include "any use of an artificial intelligence system to generate any content, decision, prediction, or recommendation concerning a consumer that is used as a basis to make a consequential decision concerning the consumer".[63] Consequential decision is defined as "a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: (a) education enrollment or an education opportunity; (b) employment or an employment opportunity; (c) a financial or lending service; (d) an essential government service; (e) health-care services; (f) housing; (g) insurance; or (h) a legal service".[64]

---

[58] An Act concerning consumer protections in interactions with artificial intelligence systems, Colorado Senate Bill 24-205 (SB 24-205) (hereinafter *Colorado AI Act*).

[59] An Act relating to regulation of the use of artificial intelligence systems in this state; providing civil penalties, Texas House Bill 149 (H.B. 149) (hereinafter *Texas AI Act*), available at https://capitol.texas.gov/tlodocs/89R/billtext/pdf/HB00149F.pdf#navpanes=0.

[60] *Colorado AI Act*, 6-1-1701(2).

[61] *Colorado AI Act*, 6-1-1701(9)(a).

[62] *Colorado AI Act*, 6-1-1701(11)(a).

[63] *Colorado AI Act*, 6-1-1701(11)(b).

[64] *Colorado AI Act*, 6-1-1701(3).

In many ways, the Colorado AI Act is very limited in scope both in terms of needing a "high-risk" use of artificial intelligence combined with its use in eight delineated areas of society. Lower risk uses of artificial intelligence are not governed by the law, and as such, remain unregulated unless they fall into another regulatory regime (such as healthcare or consumer data privacy laws).

In June 2024, Texas adopted the Texas Responsible Artificial Intelligence Governance Act, which is primarily aimed at "facilitat[ing] and advanc[ing] the responsible development and use of artificial intelligence systems".[65] The Texas AI Act is intended to (1) protect individuals and groups of individuals from known and reasonably foreseeable risks associated with artificial intelligence systems; (2) provide transparency regarding risks in the development, deployment, and use of artificial intelligence systems; and (3) provide reasonable notice regarding the use or contemplated use of artificial intelligence systems by state agencies.[66]

The Texas AI Act applies broadly to any person who: "(1) promotes, advertises, or conducts business in this state; (2) produces a product or service used by residents of this state; or (3) develops or deploys an artificial intelligence system in this state".[67] It creates a "regulatory sandbox" that "enables a person to obtain legal protection and limited access to the market in this state to test innovative artificial intelligence systems without obtaining a license, registration, or other regulatory authorization".[68] In this way, the Texas AI Act is attempting to strike a balance between protecting individuals from higher risk uses of AI while also allowing for innovation in this more fluctuating time of artificial intelligence development.

California has taken a different approach to regulating artificial intelligence than Colorado and Texas. First, instead of focusing on a more comprehensive artificial intelligence regulation, it has attempted (with marginal success) in adopting smaller, more specific artificial intelligence regulation in nuanced areas. For example, in January 2025, eighteen (18) laws related to AI went into effect in California. These laws fall, generally, into six categories.

First, California enacted two (2) general laws that create a standard definition of artificial intelligence in California and outline documentation requirements for the training and development of artificial intelligence models.[69] Second, California enacted eight (8) laws that are intended to protect individuals against certain use-cases of artificial intelligence, including protecting performers' rights, extending existing laws to protect against child sexual abuse materials with AI-generated materials and the use of deceptive AI-generated content in the political context, and prohibiting the use of non-consensual deepfake pornography.[70]

---

[65] *Texas AI Act*, Sec. A551.003(1).
[66] *Texas AI Act*, Sec. A551.003(1).
[67] *Texas AI Act*, Sec. A551.002.
[68] *Texas AI Act*, Sec. A553.051.
[69] AB 2885, available at https://legiscan.com/CA/text/AB2885/id/3020074 and AB 2013, available at https://legiscan.com/CA/text/AB2013/id/3019237 (last visited 30/09/2025).
[70] AB 1831 (child pornography laws), AB 1836 (unauthorized use of digital replicas of deceased persons without consent), AB 2602 (unauthorized use of digital replicas), AB 2655 (materially deceptive election-related content), AB 2839 (deceptive AI generated content in election advertisements), AB 2355 (clear disclosures on political advertisements for AI generated content), SB 926 (criminalizing non-consensual deep fake pornography) and SB 981 (reporting tools for social media companies).

Third, California adopted two laws that directly address the use of artificial intelligence in the healthcare context. AB 3030 requires that healthcare providers disclose to patients the use of artificial intelligence technologies in patient communications and provide patients with instructions on how to reach out to a human healthcare provider.[71] SB 1120 requires that only physicians, and not artificial intelligence technologies, can make final decisions in relation to a patient's care and treatment.[72]

Fourth, California adopted two laws that relate to their prior existing privacy legislation, the California Consumer Privacy Act (CCPA),[73] clarifying the intersection of data privacy and artificial intelligence technologies. SB 1223 clarifies that neural data is considered sensitive personal information under the CCPA, and as such, receives heightened protections under the privacy law.[74] This is relevant in the artificial intelligence context as it will require express consent from a user to use neural data with any artificial intelligence technologies. AB 1008 expressly states that AI-generated content could be considered personal information if it can be used to identify an individual.[75] As such, the consumer data rights outlined under the CPPA apply equally to artificial intelligence systems that may be ingesting personal information of California consumers and requires that deployers of artificial intelligence build in the capability to respond to those data rights as required under the CCPA.

Fifth, California adopted two laws that relate to AI transparency. SB 942 requires that "covered providers" of artificial intelligence technologies provide users with free artificial intelligence detection tools to allow users to identify whether content was generated or altered by AI technologies.[76] This transparency initiative is intended to give users control to identify if what they are viewing online or any context is real or created by artificial intelligence. AB 2905 relates to the use of artificial voices in auto-dialing technologies.[77] Specifically, companies must notify an individual, in a real voice, that the following message was created by an AI-generated voice.

Finally, the last group of enacted laws relate to the use of artificial intelligence technologies in the government and school settings. SB 896 requires that the California government assess the impact of AI on its critical infrastructure and to provide annual reports to the California legislature.[78] AB 2876 requires that AI-literacy be incorporated into the K-12 education curriculum.[79] And, SB 1288 requires the establishment of a working group to assess the safe and effective use of AI in public schools.[80]

---

[71] AB 3030, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB3030 (last visited 30/09/2025).

[72] SB 1120, available at https://legiscan.com/CA/text/SB1120/id/3023335 (last visited 30/09/2025).

[73] Cal. Civ. Code § 1798.100 et seq., as amended.

[74] SB 1223, available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1223 (last visited 30/09/2025).

[75] AB 1008, available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1008 (last visited 30/09/2025).

[76] SB 942, available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942 (last visited 30/09/2025).

[77] AB 2905, available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2905 (last visited 30/09/2025).

[78] SB 896, available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB896 (last visited 30/09/2025).

[79] AB 2876, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2876 (last visited 30/09/2025).

[80] SB 1288, available at https://legiscan.com/CA/text/SB1288/id/2981356 (last visited 30/09/2025).

Taken together, these newly enacted laws demonstrate a concerted effort to address artificial intelligence in California, even if it creates a more patchwork regulatory approach. In addition to these newly enacted laws, the California Privacy Protection Agency (CPPA) recently adopted regulations related to automated-decision making technology (ADMT).[81] The CPPA authority is limited to enforcing and providing guidance under the CPPA, so its regulations inherently relate to the overlap between ADMT and personal information.

The ADMT regulations define ADMT as "any technology that processes personal information and uses computation to replace human decision making or substantially replace human decision making".[82] By its very definition, it is limited to processing of personal information, an area already regulated within California. The ADMT Regulations create rights for consumers to (1) request to access information related to the use of ADMT technologies and the impact on the consumer; and (2) appeal any decision of the business to use ADMT for a significant decision.[83]

The ADMT Regulations outline certain requirements for any business that is using ADMT. First, the business must provide a "Pre-use notice" of any ADMT technologies to the consumer that also includes a link for the consumer to opt-out of the use of ADMT for processing the consumer's personal information.[84] These "Pre-use notices" must be "presented prominently and conspicuously to the consumer at or before the point when the business collects the consumer's personal information that the business plans to process using ADMT".[85]

Further, businesses are required to conduct risk assessments for any use of ADMT for a "significant decision concerning a consumer" or when the business will use a consumer's personal information for training an ADMT to make a significant decision regarding consumers.[86] For these risk assessments regarding ADMT, the business must identify "(i) [t]he logic of the ADMT, including any assumptions or limitations of the logic; and (ii) [t]he output of the ADMT, and how the business will use the output to make a significant decision".[87] And, the business must document the policies, procedures, and training in place "to ensure that the business's ADMT works as intended for the business's purpose and does not unlawfully discriminate based upon protected characteristics".[88] These risk assessments apply to businesses that are leveraging ADMT as well as suppliers of ADMT, who must provide sufficient

[81] California Privacy Protection Agency, *Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies*, available at https://cppa.ca.gov/regulations/ccpa_updates.html (hereinafter *ADMT Regulations*) (last visited 30/09/2025). These ADMT Regulations were adopted by the CPPA board during its July 24, 2025 meeting and approved by the California Office of Administrative Law (OAL) on September 23, 2025. *See*, CPPA, *California Finalizes Regulations to Strengthen Consumers' Privacy*, September 23, 2025, available at https://cppa.ca.gov/announcements/2025/20250923.html (last visited 30/09/2025).

[82] CCPA, *Modified text of proposed regulations*, available at https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf (last visited 30/09/2025).

[83] *ADMT Regulations*

[84] *ADMT Regulations*, 20.

[85] *ADMT Regulations*, 102.

[86] *ADMT Regulations,* 84-85.

[87] *ADMT Regulations*, 89.

[88] *ADMT Regulations*, 92.

information to allow a business using the ADMT to conduct a sufficient risk assessment as required under the Regulations.[89]

Overall, while the U.S. federal government is not taking proactive regulatory measures, the U.S. states are filling that void with a variety of approaches to artificial intelligence regulation. While the state-focused approach provides a unique opportunity to 'test' different regulatory approaches, this will prove challenging with artificial intelligence, which is impactful across borders and the globe, and so heavily reliant on large multinational companies for its development and deployment.

3. A Comparison of the Regulatory Approaches to Artificial Intelligence in the EU and the U.S.

Artificial intelligence regulation stands at a unique tipping point, bringing in legal components, geopolitical risks, and economic factors. The comparison between the approach between the EU and the U.S. is illustrative of this decisive moment. On the one hand, the U.S. is home to three out of the four most dominant AI models currently available: OpenAI with its ChatGPT; Google's Gemini; and Microsoft's Co-Pilot.[90] DeepSeek, developed and deployed out of China, is one of the only main competitors to these U.S. power houses.[91] Additionally, the U.S. is home to Nvidia, one of the dominant developers and manufacturers of semi-conductor chip technology that is a critical component of any of these large-scale AI models.[92]

The EU has none of these factors in play. While there are rapid attempts to encourage the development of artificial intelligence within Europe, it is not yet at a level where it is competing on a global stage.[93] France is an outlier in actively developing global artificial intelligence models.[94] Instead, the EU, in many ways, appears to heading towards a future where it is a buyer and user of artificial intelligence technologies that are developed elsewhere, putting it in a unique position of not having direct sovereignty over these technologies, but being highly impacted by their development and guardrails (or lack thereof).

These geopolitical tensions cannot be overstated. In the United States, the current regulatory stance toward the technology sector reflects an ongoing tension between preserving space for innovation and responding to growing demands for oversight, particularly in areas like artificial intelligence, data privacy, and technology governance. Federal policy, particularly under the Biden administration, has leaned toward a 'precision regulation' approach-seeking to target high-risk technologies and use cases without stifling broader innovation. This is evident in initiatives like the 2023 AI Executive Order, which emphasized safety, transparency, and equity, while delegating much of the implementation to sector-specific agencies and voluntary frameworks.

---

[89] *Ibid.*

[90] N. Maslej, L. Fattorini, R. Perrault, Y. Gil, V. Parli, N. Kariuki, E. Capstick, A. Reuel, E. Brynjolfsson, J. Etchemendy, K. Ligett, T. Lyons, J. Manyika, J.C. Niebles, Y. Shoham, R. Wald, T. Walsh, A. Hamrah, L. Santarlasci, J.B. Lotufo, A. Rome, A. Shi, S. Oak, *The AI Index 2025 Annual Report*, Section 1.3, AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, April 2025, *available at* https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf (hereinafter, *Standford Report*).

[91] *Ibid.*

[92] Nvidia, Contact Us, available at https://www.nvidia.com/en-us/contact/ (last visited 30/09/2025).

[93] *Stanford Report*, Section 1.3.

[94] *Stanford Report*, Section 1.3.

In many ways, the U.S. states appear to be adopting a similar "precision regulation" approach. The two comprehensive artificial intelligence laws currently enacted, Colorado and Texas, are arguably not even comprehensive in that they are focused on higher risk use cases or very narrow areas of artificial intelligence usage. And, for states where no comprehensive artificial intelligence law is enacted, or even being discussed, they are leveraging privacy laws or general consumer protection laws to create some level of guardrails for AI development and deployment. This is best exemplified by California.

At the same time, there's palpable hesitation in Congress to enact sweeping regulatory regimes that might inadvertently hamper U.S. competitiveness, especially relative to China and the EU. As a result, much of the regulatory momentum has shifted to the states and to agency rulemaking, creating a patchwork environment where companies navigate a complex web of evolving standards and requirements. This federal ambivalence reflects a broader ideological divide-balancing the historical American preference for market-driven growth with the rising awareness that unchecked technological advancement can pose systemic risks to civil liberties, economic equity, and democratic institutions.

4. How to Think About How to Regulate Artificial Intelligence

The question remains: should governments regulate artificial intelligence, even as its impacts are still unknown? Or should artificial intelligence be allowed to innovate with very few restrictions, in a wait-and-see regulatory approach?

To answer this question would require a crystal ball. Instead, it is beneficial, taking into context the EU and U.S. divergent approaches, to instead consider lessons learned from these first influential years, and how to frame out the discussion of creating controls and expectations in the next phase of artificial intelligence, and ways to inform future regulatory decision making.

4.1. Lesson Number One: Existing Laws Do Provide Some Regulatory Protections, Without Even Mentioning Artificial Intelligence

There are examples, both in the U.S. and Europe, of existing regulatory regimes that provide certain protections and requirements in the context of artificial intelligence, beyond any AI-specific regulations. The best example is data privacy. Where personal information is ingested, or anyway used by an artificial intelligence model, in both the U.S. and Europe, there are privacy requirements that will attach to that use.

In Europe, the European Data Protection Board (EDPB), which oversees EU-wide enforcement of the GDPR, issued a statement on the role of data protection authorities in the EU AI Act.[95] In that statement, the EDPB makes clear that is already actively enforcing GDPR in the context of AI technologies:

> In fact, the processing of personal data (which is often strictly intertwined with non-personal data) along the lifecycle of AI systems – and particularly along the lifecycle of those AI systems presenting a high risk to fundamental rights – clearly is (and will continue to be) a core element of the various technologies covered under the umbrella of the AI definition, as enshrined in Article 3(1) AI Act. For

[95] Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, adopted July 16, 2024, available at https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf (hereinafter, *EDPB Statement*).

> these reasons, national data protection authorities (hereinafter DPAs) have been active with regard to these technological developments9 and the EDPB, which has closely followed the legislative process regarding the AI Act10, has already initiated the examination of its (multifaceted) interplay with EU data protection law.[96]

The statement further clarifies that "whenever a general-purpose AI model or system entails the processing of personal data, it may fall – like any other AI system – under the supervisory remit, as applicable, of the relevant national DPAs (also cooperating according to Chapter VII of the GDPR) and of the EDPS (when it falls under the EUDPR)".[97] As such, even without the EU AI Acts adoption, artificial intelligence technologies are already subject to at least the GDPR when operating within or available to Europeans.

Similarly, in the U.S., as outlined in Section II, both the OCR, under HIPAA, and the FTC are actively leveraging their respective regulatory authority to oversee the use of artificial intelligence in their areas of authority. OCR issued guidance for instances where artificial technologies are used in healthcare context or leveraging protected health information in any capacity. The FTC made clear, and continues to make clear, that any commercial use of artificial intelligence must not result in unfair or deceptive trade practices. Additionally, U.S. states are using their own regulations, such as comprehensive data privacy laws and consumer protection laws, to require certain protections in the use of artificial intelligence. Combined, these measures negate a claim that artificial intelligence is completely unregulated in the U.S. In fact, it is subject to certain regulatory oversight, just not with a stand stand-alone artificial intelligence regulation.

In both the EU and the U.S., regulators should maximize the ability to leverage the existing legal infrastructures to place guardrails on the development of artificial intelligence technologies. While these may leave gaps in certain industries or use cases, they are already in place, today, making them the most effective path forward to oversee certain aspects of artificial intelligence.

4.2. Lesson Number Two: Technical Standards and Controls May Offer a Middle Ground, With Flexibility and Ease of Adoption

Technical standards and controls are a policy option that avoids the burdens and drawn-out processes of regulation but create expectations around artificial intelligence. On the U.S. side, NIST best exemplifies this approach with the AI RMF. Passing legislation in Congress would require political and strategic hurdles, no more so than in the current political environment. To avoid those challenges, voluntary technical controls and standards can fill the gap and create a de facto baseline of reasonableness.

In addition to NIST, the International Organization for Standardization (ISO) developed numerous standards addressing artificial intelligence.[98] The ISO standards address a variety of aspects of artificial intelligence, including key concepts and terminology,[99] management of artificial intelligence,[100] AI

[96] *Ivi,* 4.
[97] *Ivi,* 14.
[98] ISO, *Artificial Intelligence*, available at https://www.iso.org/sectors/it-technologies/ai (last visited 30/09/2025).
[99] ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology,* 2022.

system impact assessments,[101] artificial intelligence risk management,[102] and AI system life-cycle processes.[103] ISO standards, unlike NIST, are auditable and provide certifications of compliance, requiring that organizations demonstrate compliance to third-parties in order to affirmatively state compliance with the ISO standard.

While neither the NIST nor ISO standards are mandatory from a regulatory perspective, they are often used in the private sector for businesses to demonstrate a certain level of maturity in reasonable controls in the use of technologies. For example, businesses will often expressly state compliance with one (or both) of these standards in contracts, making voluntary standards from a regulatory standpoint now mandatory from a contractual standpoint. As more businesses are beginning to use and integrate artificial intelligence into their daily operations, business are increasingly requiring artificial intelligence developers and vendors to enter into contracts that use one of these standards to set the baseline expectations for how the tools will function and what protections will be in place for a business. As such, where regulation may lag behind, the private sector market forces may push artificial intelligence technologies to adopt certain controls and safeguards due to customer demands and contractual requirements.

4.3. Lesson Number Three: The Development of Artificial Intelligence Is Isolated to Only a Few Regions in the World

As artificial intelligence continues to develop, the U.S. and China are dominating the development of these tools and technologies. With the clustering of artificial development, and the technological infrastructure to support that development, into such few areas, it becomes even more important for these regions to create a harmonized approach to overseeing the development and use of artificial intelligence tools.

The geographic concentration of artificial intelligence development in the U.S. and China[104] will profoundly shape the regulatory landscape in both the U.S. and Europe. In the U.S., the dominance of domestic artificial intelligence companies creates strong economic and geopolitical incentives to maintain a more permissive regulatory environment. Lawmakers, especially at the federal level, appear particularly focused on the fear that stringent rules could weaken the global competitiveness of U.S. tech companies vis-à-vis their Chinese counterparts. As a result, U.S. regulation is likely to remain sectoral, fragmented, and innovation-friendly, with an emphasis on voluntary standards, soft law, and targeted interventions rather than sweeping statutory frameworks. The concentration of corporate power in a handful of American firms also ensures that industry voices exert significant influence over the regulatory agenda, reinforcing this cautious approach.

In Europe, by contrast, the absence of globally competitive artificial intelligence solutions fuels a different set of incentives. European regulators, recognizing their comparative weakness in artificial intelligence innovation, have positioned themselves as global leaders in artificial intelligence

[100] ISO/IEC 42001, *Information technology — Artificial intelligence — Management system*, 2023.
[101] ISO/IEC 42005, *Information technology — Artificial intelligence (AI) — AI system impact assessment*, 2025.
[102] ISO/IEC 23894, *Information technology — Artificial intelligence — Guidance on risk management*, 2023.
[103] ISO/IEC 5338, *Information technology — Artificial intelligence — AI system life cycle processes*, 2023.
[104] *See*, *supra*, note 90.

governance, much as Europe did with data protection. By setting ambitious standards — such as the EU AI Act — the EU seeks to exercise 'normative power', exporting its regulatory model extraterritorially and shaping the practices of U.S. and Chinese firms that wish to access the European market. The reliance on external artificial intelligence technologies also magnifies European concerns about sovereignty, dependence, and the protection of fundamental rights, all of which drive a more precautionary, rights-oriented regulatory framework.

These unique dynamics mean that the global approach to artificial intelligence regulation will be shaped by a triangular interplay: U.S. regulators protecting domestic innovators, EU regulators projecting values-based governance outward, and China pursuing state-led strategies that blend technological development with political control.[105] The result is not a harmonized system, but a fragmented and competitive regulatory environment, in which Europe attempts to wield rule-making authority, the U.S. prioritizes innovation and competitiveness, and both must ultimately reckon with the reality that the technological frontier is being set largely outside of Europe. This asymmetry will continue to shape both the form and ambition of regulatory initiatives across the Atlantic.

5. Conclusion

There is no right answer to when and how to regulate any emerging technology – and artificial intelligence is no different. However, artificial intelligence does pose unique challenges by its very nature as an incredible powerful tool and its rapid adoption by users across the globe. The regulatory trajectories of the EU and the U.S. reflect not merely divergent legal traditions but fundamentally different philosophies of technology governance. The EU, through its comprehensive EU AI Act, embraces a precautionary and risk-based framework that prioritizes fundamental rights and harmonized obligations across member states. By contrast, the U.S. leans toward sector-specific and innovation-driven approaches, emphasizing guidance, self-regulation, and adaptive enforcement rather than an overarching statutory regime. Each system responds to its own institutional logic: the EU's deep-rooted emphasis on rights protection and market integration, and the U.S.'s preference for flexibility, competitiveness, and decentralized oversight.

Yet, these differences also underscore valuable lessons. From the EU, policymakers can see the benefits of legal certainty, uniformity, and proactive safeguards in cultivating public trust. From the U.S., the value of flexibility, experimentation, and avoiding premature over-regulation becomes evident, ensuring that technological innovation is not unduly stifled. The juxtaposition highlights the tension between fostering innovation and protecting society, a balance that all jurisdictions must carefully navigate.

Ultimately, the future of artificial intelligence regulation will likely require hybridization: combining the EU's structured rights-based protections with the U.S.'s adaptive and sectoral responsiveness. As artificial intelligence becomes a global technology, transatlantic convergence — or at least interoperability — will be crucial to avoid fragmentation, ensure accountability, and preserve both innovation and human dignity. The comparative experience suggests that the most effective regulatory path forward lies not in rigid adherence to one model, but in the dialogue between them.

[105] ZHANG, A. HUYUE, *The Promise and Perils of China's Regulation of Artificial Intelligence*, in *Columbia J. Trans.*, 2025, 5-6.