

2023

Should the United States Adopt Federal Artificial Intelligence Regulation Similar to the European Union

Jean Joseph
Loyola University Chicago Law School

Follow this and additional works at: <https://lawecommons.luc.edu/lucilr>



Part of the [Civil Rights and Discrimination Commons](#), [Computer Law Commons](#), [International Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

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 (2023).

Available at: <https://lawecommons.luc.edu/lucilr/vol20/iss1/5>

This Student Article is brought to you for free and open access by LAW eCommons. It has been accepted for inclusion in Loyola University Chicago International Law Review by an authorized editor of LAW eCommons. For more information, please contact law-library@luc.edu.

SHOULD THE UNITED STATES ADOPT FEDERAL ARTIFICIAL INTELLIGENCE REGULATION SIMILAR TO THE EUROPEAN UNION

Jean Joseph*

Abstract

Artificial Intelligence (AI) promises to revolutionize our everyday lives and how we approach all sectors of the economy and society. For the laundry list of benefits this form of technology provides, there is a concern as to the ways AI can produce troubling outcomes – including racial discrimination and social inequality. The United States House of Representatives introduced the National AI Initiative Act of 2020 (NAIIA) to ensure continued US leadership in AI research and development. However, the NAIIA leaves issues concerning the risk of biases and discrimination associated with using AI systems to federal agencies and state governments. While promoting similar objectives, the European Union’s (EU) AI Act ensures that AI systems used in the market are safe and respect existing laws on fundamental rights. This Comment argues that American lawmakers should look to the EU’s AI Act as a model for enacting federal legislation that ensures AI systems used in the public and private sectors are safe and do not infringe on an individual’s fundamental rights.

First, the Comment reviews the history of AI, AI legislation in the United States at the federal and state level, and the EU’s AI Act. Next, the Comment analyzes the strengths and weaknesses of the European Union’s AI Act, the National AI Initiative Act, and potential biases, discrimination, and racial inequality concerns under the present framework of AI regulation in the United States. Finally, the Comment argues that the United States should borrow the favorable provisions from the EU’s AI Act, improve upon its weaknesses, and pass comprehensive federal AI legislation that emphasizes the fundamental rights of individuals while simultaneously promoting investment in AI research and development necessary to maintain US leadership in this form of technology.

Table of Contents

| | |
|-------------------------------------------------------|-----|
| I. Introduction | 106 |
| II. Background | 107 |
| A. The History of Artificial Intelligence | 107 |
| B. Racial Biases in Artificial Intelligence | 109 |
| III. Discussion | 110 |
| A. Overview of the EU AI Act | 110 |

* Jean Joseph is a third-year law student at Loyola University Chicago School of Law, Class of 2024.

Should the United States Adopt AI Regulation

B. Overview of High-Risk AI Systems 111
C. EU AI Act Fundamental Rights Concerns 113
IV. Analysis 115
A. National Artificial Intelligence Initiative Act 115
B. Bias, Discrimination, and Social Inequality
Concerns Under Current U.S. AI Regulation 116
V. Proposal 120
A. Amendments to the National Artificial Intelligence
Initiative Act 120
B. Expanded Role for the National Artificial Intelligence
Advisory Committee 121
V. Conclusion 122

I. Introduction

On April 21, 2021, the European Commission (Commission) proposed the Artificial Intelligence Act (EU AI Act), which, if adopted, would provide a framework for the governance of artificial intelligence (AI) in the European Union (EU).¹ The proposed AI Act aims to diminish the differences between national rules and create one common regulatory framework for the entire EU.² Through the EU AI Act, the Commission aims to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values, ensure legal certainty to facilitate investment and innovation in AI, enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems, and facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.³ One of the EU AI Act’s objectives is to foster legal certainty and provide safeguards for human-centric technologies that internalize European values, as enshrined in the European Charter of Fundamental Rights, the European Convention of Human Rights, and the European AI Ethics Guidelines.⁴

In October 2016, the White House Office of Science and Technology Policy (OSTP) released a series of reports defining the federal government’s role in the development of AI as a facilitator of innovation and a minimalist regulator.⁵ Also, it outlined how federal research and development investments would guide the “long term transformational impact of AI.”⁶ The National AI Initiative

¹ *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final, (Apr. 21, 2021) (hereafter, EU AI Act).

² Natali Helberger & Nicholas Diakopoulos, *The European AI Act and How It Matters for Research into AI in Media and Journalism*, DIGITAL JOURNALISM 1, 2 (2022).

³ EU AI Act, *supra* note 1.

⁴ *Ethics Guidelines for Trustworthy AI*, EUR. COMM’N (Nov. 17, 2022), <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

⁵ Corinne Cath et al., *Artificial Intelligence and the ‘Good Society’: the US, EU, and UK approach.*, 24 SCI. ENG. ETHICS 506, 510 (2018).

⁶ *Id.*

Should the United States Adopt AI Regulation

Act of 2020 (NAIIA) became law on January 1, 2021.⁷ The NAIIA's focuses on improving AI innovation, advancing trustworthy AI, creating new education and training opportunities through AI, improving existing infrastructure through new technologies, facilitating federal and private sector utilization of AI to improve existing systems, and promoting an international environment that supports further advances in AI.⁸ A critical difference between the EU AI Act and the NAIIA is that the NAIIA leaves issues concerning the risk of biases and discrimination associated with using AI systems to federal agencies and state governments. Instead of including language within the NAIIA which ensures AI systems placed and used in the US market are safe and respect existing laws on fundamental rights, the NAIIA mandates the establishment of a subcommittee for AI and law enforcement that advises on biases and other fundamental rights concerns. American lawmakers should look to the EU AI Act as a model for enacting federal legislation that ensures AI systems used in the public and private sectors are safe and do not infringe on an individual's fundamental rights.

Part I of this Comment reviews the history of AI and how AI perpetuates social prejudices and injustices. Part II discusses the EU's AI Act, high-risk AI systems, and fundamental rights concerns. Part III analyzes the strengths and weaknesses of the EU AI Act, the NAIIA, and potential biases, discrimination, and racial inequality concerns under the present framework of AI regulation in the US. Part IV argues that the US should borrow the favorable provisions from the EU AI Act, improve upon its weaknesses, and pass comprehensive federal AI legislation that emphasizes the fundamental rights of individuals while simultaneously promoting investment in AI research and development necessary to maintain US leadership in this form of technology.

II. Background

A. The History of Artificial Intelligence

Modern AI traces back to the 1950s when Alan Turing published "Computing Machinery and Intelligence," where he described how to create intelligent machines and how to test their intelligence.⁹ The article led to what later became known as "The Turing Test," which measured a machine's ability to think as a human would.¹⁰ The Turing Test asks, "if a human is interacting with another human and a machine and unable to distinguish the machine from the human, then the machine is said to be intelligent."¹¹ In 1956, John McCarthy created

⁷ H.R. REP. NO. 116-617 (2021) (Conf. Rep.).

⁸ *Id.*

⁹ See generally Michael Haenlein & Andreas Kaplan, *A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence*, 61 CAL. MGMT. REV. 5 (2019).

¹⁰ Rebecca Reynoso, *A Complete History of Artificial Intelligence*, G2 (May 25, 2021), <https://www.g2.com/articles/history-of-artificial-intelligence>.

¹¹ Haenlein, *supra* note 9.

Should the United States Adopt AI Regulation

the word “Artificial Intelligence at the Dartmouth Summer Research Project on Artificial Intelligence (DSRP AI) workshop at Dartmouth College.¹² Following the workshop, Allen Newell and Herbert Simon created Logic Theorist, the first AI computer program capable of reasoning by proving theorems starting from mathematical principles.¹³ Success continued into the 1960s due to the creation of new programming languages, robots, and research findings.¹⁴ In 1961, Unimate became the first robot to work on a General Motors assembly line.¹⁵ In 1965, Joseph Weizenbaum developed ELIZA, an interactive computer program that could communicate in English with a human being.¹⁶

Unfortunately, the 1970s were not as promising. Commonly known as the “AI Winter,” this period saw a sharp decline in government funding on AI research.¹⁷ For the next two decades, innovation in the field of artificial intelligence remained relatively stagnant in comparison to the prior years. However, the 1990s and 2000s gave way to machine learning AI applications.¹⁸ For example, in 1997, Sepp Hochreiter and Jürgen Schmidhuber developed the Long Short-Term Memory (LSTM), which is a type of recurrent neural network (RNN) architecture used for handwriting and speech recognition.¹⁹ In the same year, IBM’s Deep Blue chess-playing program became the first system to beat a reigning world champion.²⁰ In 2000, Professor Cynthia Breazeal developed Kismet, a robot that could recognize and simulate emotions with its face.²¹ In 2002, i-Robot released Roomba²², which is now a staple in many households. In 2004, NASA’s Spirit and Opportunity rovers navigated Mars’ surface without human intervention.²³

From smartphones to home electronics, AI has become a part of our everyday lives. In 2010, Microsoft launched Kinect for Xbox 360, which is the first gaming device that tracked human body movement using a 3D camera and infrared detection.²⁴ In 2011, IBM’s Watson, a natural language question-answering computer, defeated two former “Jeopardy!” champions.²⁵ In 2011, Apple released Siri.²⁶ A few years later, Microsoft released Cortana, Amazon created Amazon

¹² Reynoso, *supra* note 10.

¹³ Lucrezia Fanti et al., *From Heron of Alexandria to Amazon’s Alexa: A Stylized History of AI and its Impact on Business Models, Organization and Work*, 49 J. IND. BUS. ECON. 409, 415 (2022).

¹⁴ Reynoso, *supra* note 10.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ Haenlein, *supra* note 9.

¹⁸ Reynoso, *supra* note 10.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ Reynoso, *supra* note 10.

²⁵ *Id.*

²⁶ *Id.*

Should the United States Adopt AI Regulation

Alexa, and Google released Google Home.²⁷ In 2016, “Sophia” became the first “robot citizen” capable of performing image recognition, make facial expressions, and communicate through AI.²⁸ A major accomplishment in AI innovation occurred in 2015 when AlphaGo, a program developed by Google, was able to beat the reigning world champion in the board game Go.²⁹ AlphaGo achieved this success utilizing deep learning, a form of AI applied in image recognition algorithms used by Facebook and speech recognition algorithms that fuel smart speakers and self-driving cars.³⁰

B. Racial Biases in Artificial Intelligence

Our preferences and biases shape the way we perceive the world around us. Our biases may lead to the exclusion, marginalization, or targeting of racial/ethnic groups. Although AI can improve efficiency and reduce human error, it can also perpetuate social prejudices and injustices.³¹ The causes for bias are both technical and social: the code can be embedded through the biases of the designers and data, and the use of AI can exacerbate bias already existing in a social system.³² Federal agencies are increasingly adopting and delegating decision-making responsibilities to AI technology.³³ AI systems are models used to form predictions based on patterns learned in historical data.³⁴ Designers choose which dataset the model will learn from, determine the accuracy of the model’s prediction for different groups, and the testing procedure to evaluate the model.³⁵ Next, users determine whether the AI model is appropriate for their task, how to use the AI predictions, and who will manage the AI³⁶ Finally, users act on the predictions, choose how to manage the AI system, and use the results to make decisions with the immediate impact.³⁷ It is through this process that without sufficient safeguards, our decisions can incorporate racial bias into AI systems, causing significant impact.³⁸

²⁷ *Id.*

²⁸ *Id.*

²⁹ Haenlein, *supra* note 9.

³⁰ *Id.*

³¹ Morgan Livingston, *Policy Memo: Preventing Racial Bias in Federal AI*, J. SCI. POL’Y & GOVERNANCE (May 27, 2020).

³² *Id.*

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

Should the United States Adopt AI Regulation

III. Discussion

A. Overview of the EU AI Act

The Act defines an “AI system” as software that is developed using specific techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.³⁹ As stated in Annex I, the techniques and approaches referred to are “Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning,” “Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;” and “Statistical approaches, Bayesian estimation, search and optimization methods.”⁴⁰

The Act provides horizontal regulation of AI systems consistent with existing EU human rights legislation and laws regulating data protection, data governance, consumer protection, non-discrimination, and gender equality.⁴¹ Utilizing a risk-based approach, the Act sets out the minimum necessary requirements to address risks to values, fundamental rights, and principles associated with AI development and deployment without unnecessarily constraining technological development or trade.⁴² Furthermore, the Act would have an extraterritorial effect, meaning that it would apply to users of AI systems in the EU and providers placing on the market or putting into service AI systems in the EU, irrespective of whether those providers are established within the EU or in a third country.⁴³ Its impact would be felt across the economy, creating new regulatory obligations for AI tools used in financial services, education, employment and human resources, law enforcement, industrial AI, medical devices, the car industry, machinery, and toys.⁴⁴

The Act prohibits systems that pose an unacceptable risk, sets standards for systems that pose a high risk to fundamental rights, requires enhanced transparency for systems that pose a limited risk, and limits systems that pose a minimal risk to a voluntary code of conduct.⁴⁵ The Act prohibits AI systems that use subliminal techniques that are beyond a person’s consciousness to materially

³⁹ EU AI Act, *supra* note 1, art. 3(1).

⁴⁰ *Annexes to the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final*, (Apr. 21, 2021), Annexes 1 to 9 (hereafter EU AI Act Annexes), annex 1.

⁴¹ Bev Townsend, *Decoding the Proposed EU AI Act*, AM. SOC’Y INT’L L. INSIGHTS, Sept. 20, 2021, at 3.

⁴² EU AI Act, *supra* note 1, Explanatory Memorandum ¶ 3.5.

⁴³ EU AI Act, *supra* note 1, art. 2(1)(a).

⁴⁴ Benjamin Mueller, *The Artificial Intelligence Act: A Quick Explainer*, CENTER FOR DATA INNOVATION (May 4, 2021), <https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/>.

⁴⁵ Natalie 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. BIRMINGHAM, Aug. 5, 2021, at 2.

Should the United States Adopt AI Regulation

distort behavior in a way likely to cause that person physical or psychological harm.⁴⁶ The Act bans AI systems that exploit vulnerable groups to materially distort a person's behavior in a way likely to cause them harm.⁴⁷ The Act prohibits social score systems that evaluate or classify the trustworthiness of natural persons based on their social behavior, resulting in scores with a detrimental impact on those whose data were collected.⁴⁸ Moreover, the Act bans "real-time" remote biometric identification systems in publicly accessible spaces used for law enforcement, except where "strictly necessary."⁴⁹ The Act provides exceptions systems that pose an unacceptable risk depending on the potential harm caused.⁵⁰ Most AI will fall within unacceptable and minimal risk systems, however, for high-risk systems, the Act provides strict obligations before they may be put on the market.⁵¹

B. Overview of High-Risk AI Systems

High-risk systems are those "intended to be used as a safety component of a product or is itself a product" covered by specific EU product safety and conformity legislation.⁵² The Act does not clearly define a high-risk system, but it includes systems that pose a significant risk to health, safety, and fundamental rights. The Act allows for the expansion of high-risk systems without promulgating new legislation if the Commission determines that the products pose a high risk to health, safety, and fundamental rights and has the potential to affect a "plurality of persons" and the inability of end-users to opt-out of an adverse outcome.⁵³ High-risk systems are subject to a risk management system, data training and data governance, technical documentation, recordkeeping, transparency, human oversight, accuracy, robustness, and cybersecurity.⁵⁴

The risk management system must identify known and foreseeable risks, evaluate risks that occur when the AI system is in use, evaluate potential risks after implementation, and adopt appropriate risk management measures.⁵⁵ High-risk AI systems that use training of models with data would need to satisfy appropriate data governance and management practices, such as relevant design choices and data preparation processing operations, relevant assumptions with respect to the information that the data intends to measure, examine possible biases, and address potential data gaps.⁵⁶ Technical documentation of features such as the

⁴⁶ EU AI Act, *supra* note 1, art. 5(1)(a).

⁴⁷ *Id.* art. 5(1)(b).

⁴⁸ *Id.* art. 5(1)(c).

⁴⁹ *Id.* art. 5(1)(d).

⁵⁰ Smuha et al, *supra* note 45.

⁵¹ *Id.*

⁵² EU AI Act, *supra* note 1, art. 6(1)(a).

⁵³ Mueller, *supra* note 44.

⁵⁴ EU AI Act, *supra* note 1, art. 16(a).

⁵⁵ *Id.* art. 9.

⁵⁶ *Id.* art. 10.

Should the United States Adopt AI Regulation

system architecture, algorithmic design, and model specifications must be drawn up before the system is placed on the market or put into service, and it must be continuously updated.⁵⁷ The high-risk AI system must include automatic logging of events while the system is running, allowing for traceability of the system's functioning throughout its lifecycle.⁵⁸ The system must also be designed in a way that ensures that operation is sufficiently transparent to allow users to interpret its output and use the system appropriately.⁵⁹ High-risk AI systems must be designed to always maintain human oversight and prevent or minimize risks to health, safety, or fundamental rights.⁶⁰ The system must also be designed in a way that achieves a consistent level of accuracy, robustness, and cybersecurity throughout its lifecycle.⁶¹

Additionally, providers of high-risk AI systems must undergo a conformity assessment before placing the system on the market or putting it into service.⁶² If the assessment shows that the requirements of the EU AI Act were satisfied, then the providers submit an EU declaration of conformity and affix the CE marking of conformity.⁶³ CE marking indicates that the manufacturer assessed the product and determined it met EU safety, health, and environmental protection requirements.⁶⁴ It is required for products manufactured anywhere in the world that are then marketed in the EU.⁶⁵ If an importer places a high-risk AI system on the market, they must verify that the provider has done the conformity assessment, drawn up the technical documentation, ensure the system bears the required conformity marking, and included the required documentation and instructions for use.⁶⁶ The Act requires systems governed by existing product safety legislation to maintain their current conformity assessment structures and regulatory frameworks.⁶⁷

The Act allows these systems to integrate existing safety legislation to avoid duplicating administrative burdens and to maintain responsibilities while ensuring consistency among the different strands of EU legislation.⁶⁸ Compliance with the EU AI Act is subject to conformity assessment procedures already established in each sector, which may not confirm whether the product satisfies the EU AI Act.⁶⁹ High-risk AI systems that are not subject to existing legislation are

⁵⁷ *Id.* art. 11.

⁵⁸ *Id.* art. 12.

⁵⁹ *Id.* art. 13.

⁶⁰ *Id.* art. 14.

⁶¹ *Id.* art. 15.

⁶² *Id.* art. 19.

⁶³ EU AI Act, *supra* note 1, art. 19.

⁶⁴ *CE Marking*, EUR. COMM'N (Nov. 11, 2022), https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm.

⁶⁵ *Id.*

⁶⁶ EU AI Act, *supra* note 1, art. 26(1).

⁶⁷ *Id.* Explanatory Memorandum ¶ 1.2.

⁶⁸ *Id.*

⁶⁹ Jakob Mökander, et al., *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation*, 32 MINDS & MACHINES 241, 248-53.

Should the United States Adopt AI Regulation

referred to as “stand-alone” systems and must comply with the requirements set out in the EU AI Act.⁷⁰ AI providers not subject to existing legislation must conduct their own conformity assessment and file their system in a database for high-risk AI systems.⁷¹

AI providers must also establish post-market monitoring systems designed to document and analyze performance of high-risk AI systems throughout their lifecycle.⁷² The post-market monitoring system links to quality management, which establishes procedures for how providers design, test, and verify high-risk AI systems.⁷³ The quality management system also includes procedures for how to implement and maintain post-market monitoring of the respective high-risk system.⁷⁴ Distributors, importers, and users are subject to provider obligations if they place a high-risk AI system on the market under their name or make a substantial modification to it.⁷⁵ Distributors and importers must verify that the high-risk AI system bears the required CE conformity marking, contains the required documentation and instruction of use, and that the provider and the importer of the system comply with their obligations under the Act.⁷⁶ Users must deploy the system correctly, ensure the input data is of high quality, and monitor the system’s performance on an ongoing basis with specific logging and audit requirements.⁷⁷ Users also need to implement a risk management system that documents and mitigates all risks associated with the AI system.⁷⁸

C. EU AI Act Fundamental Rights Concerns

The Commission’s decision to not overregulate AI systems leave too much discretion to providers to decide on fundamental rights violations. The Act limits fundamental rights to a set of safety standards without considering its uniqueness, it takes a more technical approach to preserve fundamental rights, and the Act’s risk categories are insufficient to protect fundamental rights adequately.⁷⁹ The Act limits the scope of fundamental rights protections to promote economic activity and innovation.⁸⁰ This balancing act leaves AI systems more susceptible to interferences, intrusions, and violations of fundamental rights.⁸¹

⁷⁰ EU AI Act, *supra* note 1, Explanatory Memorandum ¶ 5.2.

⁷¹ *Id.*

⁷² *Id.* art 61.

⁷³ Mökander, *supra* note 69, at 252.

⁷⁴ *Id.*

⁷⁵ EU AI Act, *supra* note 1, art. 28.

⁷⁶ *Id.* art. 26-27.

⁷⁷ *Id.* art. 29.

⁷⁸ *Id.*

⁷⁹ Smuha et al., *supra* note 45.

⁸⁰ *Id.*

⁸¹ *Id.*

Should the United States Adopt AI Regulation

Regulations placed on providers of high-risk systems fail to promote the Commission's goal of offering a high level of protection for fundamental rights.⁸² The discretion given to providers, the existing enforcement standards, and the remedies available lacks the level of scrutiny and oversight necessary to ensure sufficient protection against the dangers AI systems pose to the fundamental rights of those living in the EU.⁸³ For instance, the EU AI Act states that high risk system must be sufficiently transparent to ensure the user's ability to interpret and use the system's output.⁸⁴ However, the user is not obligated to communicate that information to persons subject to the AI supported decision.⁸⁵ AI users are also not obligated to explain or justify the decisions they reach towards those affected by them.⁸⁶ The users' only transparency obligation to persons subject to the AI is to inform them about the fact that an AI system is used.⁸⁷

By setting fundamental rights protections based on market conditions, the Act currently fails to provide a "balanced and proportionate regulatory approach that is limited to the minimum necessary requirements to address the risks and problems linked to AI."⁸⁸ The tiers of acceptable AI risk before a system enters the market is insufficient to ensure that AI providers respect fundamental rights. The Act treats AI systems similarly to products such as cars, machinery, and toys.⁸⁹ This ignores the seriousness of these applications and the societal consequences if used improperly.

Rather than prohibiting AI systems that violate fundamental rights, the Act prohibits systems that engage in practices that create an "unacceptable risk."⁹⁰ The remaining risk categorizations allow for a degree of interference with fundamental rights if AI providers adhere to a voluntary code of conduct, enhanced transparency, set standards for systems that pose a high risk, and a system of self-assessment by AI providers.⁹¹ Only AI systems identified as high-risk by the Commission must adhere to mandatory requirements. No risk or limited risk systems require increased transparency measures, and AI providers are only obligated to inform people that they are subjected to an AI system.⁹² As a result, fundamental rights protection depends on if the Commission determines that the products pose a high risk to health, safety, and fundamental rights and has the potential to affect a "plurality of persons" and the inability of end-users to opt out of an adverse outcome.⁹³ Given how quickly AI technology is evolving,

⁸² EU AI Act, *supra* note 1, Explanatory Memorandum ¶ 1.1.

⁸³ Smuha et al., *supra* note 45.

⁸⁴ EU AI Act, *supra* note 1, art. 13.

⁸⁵ Melanie Fink, *The EU Artificial Intelligence Act and Access to Justice*, EU LAW LIVE (May 10, 2021), <https://eulawlive.com/op-ed-the-eu-artificial-intelligence-act-and-access-to-justice-by-melanie-fink/#>.

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ EU AI Act, *supra* note 1, at ¶ 1.1.

⁸⁹ Mueller, *supra* note 53.

⁹⁰ Smuha et al., *supra* note 45.

⁹¹ *Id.*

⁹² *Id.*

⁹³ EU AI Act, *supra* note 1, art. 16(a).

Should the United States Adopt AI Regulation

providing a comprehensive list of high-risk systems may be challenging. Moreover, the effectiveness of the mandatory requirements imposed on high-risk AI systems hinges on the quality of the risk management system.⁹⁴ Over time, the mandatory requirements may become less effective if AI providers who do not wish to subscribe to them can circumvent them by arguing that their system is not within the list of high-risk systems.⁹⁵

IV. Analysis

A. National Artificial Intelligence Initiative Act

The National Artificial Intelligence Act (“NAIIA”) centers on American leadership in AI research and development, the development of trustworthy AI systems, preparing for potential workforce disruptions, and coordinating military and civilian sectors.⁹⁶ The NAIIA takes a hands-off approach to the domestic governance of AI technologies focusing on limiting regulatory overreach to empower individuals and corporations to benefit from AI.⁹⁷ The NAIIA is more involved in promoting an international environment that opens markets for American AI industries, protects America’s technological advantage, and ensures that international cooperation is consistent with American values.⁹⁸

The United States’ focus on military defense and national security is the most developed aspect of its AI strategy. Prior to the NAIIA, the 2019 National Defense Authorization Act established the National Security Commission on AI, which was an independent bipartisan commission “to consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States.”⁹⁹ In its Final Report the Commission presented a strategy to reorganize the government to defend and compete in the coming era of AI-accelerated competition and conflict.¹⁰⁰ The first part of the report entitled “Defending America in the AI Era,” explains what the United States must do to defend against AI-related threats and recommends how the U.S. government can responsibly use AI technologies to protect American people and interests.¹⁰¹ The second part, “Winning the Technology Competition,” addresses the critical elements of the AI competition and recommends

⁹⁴ Smuha et al., *supra* note 45.

⁹⁵ *Id.*

⁹⁶ National Artificial Intelligence Initiative Act of 2020, 15 U.S.C. §§ 9401-9461.

⁹⁷ Huw Roberts et al., *Achieving a ‘Good AI Society’: Comparing the Aims and Progress of the EU and the US*, SCI. ENG. ETHICS, Nov. 12, 2021, at [pincite].

⁹⁸ *Id.*

⁹⁹ National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §1051, 132 Stat. 1964 (2018).

¹⁰⁰ NAT’L SEC. COMM’N A.I., FINAL REPORT [pincite] (2021).

¹⁰¹ *Id.*

Should the United States Adopt AI Regulation

actions the government must take to promote AI innovation to improve national competitiveness and protect critical U.S. advantages.¹⁰²

The NAIIA established the National AI Initiative Office (“NAIIO”), which is responsible for implementing a national AI strategy and coordinating artificial intelligence research and policymaking across government, industry, and academia.¹⁰³ The NAIIO established the AI Researchers Portal, which connects researchers to federal resources and relevant grant funding programs.¹⁰⁴ The Portal includes information about the federal grants and funding processes for researchers, a directory of active AI federal research programs that connects researchers with potential funding opportunities and collaborations, a list of federal datasets and repositories, and links to computing infrastructure programs for AI research.¹⁰⁵

The NAIIA established the National AI Research Resource Task Force (the “Task Force”).¹⁰⁶ The Task Force consists of technical experts who provide recommendations on the feasibility of establishing a National AI Research Resource (“NAIRR”).¹⁰⁷ The NAIRR is a shared data infrastructure that provides researchers access to resources necessary for continued AI research and development.¹⁰⁸ The Task Force provides recommendations for establishing the NAIRR’s technical capabilities, governance, administration, assessment and requirements for security, privacy, civil rights, and civil liberties.¹⁰⁹ The NAIIA also established the National Artificial Intelligence Advisory Committee (“NAIAC”), which advises the President and the NAIIO on matters relating to the NAIIA.¹¹⁰

B. Bias, Discrimination, and Social Inequality Concerns Under Current U.S. AI Regulation

The NAIIA focuses on improving AI innovation and trustworthiness. However, it lacks language highlighting the need to improve AI in areas that would result in differential treatment or disparate impact for vulnerable populations.¹¹¹ Excluding these considerations from the NAIIA would perpetuate existing

¹⁰² *Id.*

¹⁰³ *National AI Initiative Office Launches AI Researchers Portal*, HPCWIRE (Jan. 6, 2022), <https://www.hpcwire.com/off-the-wire/national-ai-initiative-office-launches-ai-researchers-portal/>.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *The Biden Administration Launches the National Artificial Intelligence Research Resource Task Force*, WHITE HOUSE (June 10, 2021), <https://www.whitehouse.gov/ostp/news-updates/2021/06/10/the-biden-administration-launches-the-national-artificial-intelligence-research-resource-task-force/>.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ *National Artificial Intelligence Advisory Committee (NAIAC)*, NAT’L. INST. STANDARDS & TECH. (July 13, 2023), <https://www.nist.gov/artificial-intelligence/national-artificial-intelligence-advisory-committee-naiac>.

¹¹¹ Nicol Turner Lee & Samantha Lai, *The U.S. Can Improve its AI Governance Strategy by Addressing Online Biases*, BROOKINGS (May 17, 2022), <https://www.brookings.edu/blog/techtank/2022/05/17/the-u-s-can-improve-its-ai-governance-strategy-by-addressing-online-biases/>.

Should the United States Adopt AI Regulation

historic and systemic inequalities. Housing, hiring, criminal justice, healthcare, finance, politics, and facial recognition technologies are implementing AI into their services.¹¹² These places have a history of providing poor or inadequate decisions to people of color. Having AI systems that did not consider their needs and lived experiences would further burden these communities. Suppose the federal government gets bias identification and mitigation wrong. In that case, it will erode the public's trust in the efficacy of AI systems.

People of color have always been disadvantaged in obtaining affordable housing in the United States. Rather than prevent biases, AI-based lending services have reproduced the discrimination people of color face in getting a home loan. AI has exacerbated biases in home appraisals and loan approvals for Black homeowners.¹¹³ AI-based mortgage lending systems have charged Black and Hispanic borrowers higher prices for mortgage loans.¹¹⁴ Neither study found that from 2008 to 2015, online lenders have rejected a total of 1.3 million creditworthy Black and Hispanic applicants.¹¹⁵ Even existing homeowners in majority Black neighborhoods have seen their property appraised for 23% less than those in predominantly White neighborhoods.¹¹⁶

Hiring processes have changed over the years due to the introduction of algorithms that favor White applicants over people of color.¹¹⁷ Targeted ads on social media apps for job postings skew heavily toward specific gender and racial groups depending on the job.¹¹⁸ Many employers are using emotion recognition technology (“ERT”) to evaluate candidates.¹¹⁹ ERT relies on software that observes a person's facial expressions and bodily cues.¹²⁰ However, more Black and Hispanic men have been passed over for employment when prescreened using ERT compared to their White counterparts.¹²¹

AI has reinforced the history of biased and discriminatory laws in the criminal justice system. For instance, on December 21, 2018, President Trump signed into law the First Step Act, which among other things, intended to reduce recidivism

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ Charlton McIlwain, *AI Has Exacerbated Racial Bias in Housing. Could it Help Eliminate it Instead?*, MIT TECH. REV. (Oct. 20, 2020), <https://www.technologyreview.com/2020/10/20/1009452/ai-has-exacerbated-racial-bias-in-housing-could-it-help-eliminate-it-instead/>.

¹¹⁵ Khristopher J. Brooks, *Disparity in Home Lending Costs Minorities Millions, Researchers Find*, CBS NEWS (Nov. 15, 2019, 10:59 AM), <https://www.cbsnews.com/news/mortgage-discrimination-black-and-latino-paying-millions-more-in-interest-study-shows/>.

¹¹⁶ Andre M. Perry, Jonathan Rothwell & David Harshbarger, *The Devaluation of Assets in Black Neighborhoods*, BROOKINGS (Nov. 27, 2018), <https://www.brookings.edu/research/devaluation-of-assets-in-black-neighborhoods/>.

¹¹⁷ Lee & Lai, *supra* note 111.

¹¹⁸ *Id.*

¹¹⁹ Jenn Fulmer, *The Value of Emotion Recognition Technology*, IT BUSINESS EDGE, (Sept. 21, 2021), <https://www.itbusinessedge.com/business-intelligence/value-emotion-recognition-technology/#what-is>.

¹²⁰ *Id.*

¹²¹ *Id.*

Should the United States Adopt AI Regulation

and provide inmates incentives for good behavior.¹²² To complete this objective, the Department of Justice created the Pattern algorithm to predict recidivism and shorten criminal sentences based on good behavior.¹²³ The algorithm used factors such as their criminal history, education level, and disciplinary incidents while incarcerated to determine inmates who pose a low risk of returning to crime.¹²⁴ It divided inmates into groups of people who can get credit for completing the program and get out early, and those who cannot.¹²⁵ Unfortunately, the algorithm exhibited biases against people of color, overpredicting recidivism among minority inmates at higher rates compared to White inmates.¹²⁶ Other commercial risk assessment algorithms used by state and local governments have incorrectly judged Black inmates as more likely than white inmates to be at a higher risk of recidivism, while White inmates were more likely than Black inmates to be incorrectly flagged as low risk.¹²⁷

AI has also contributed to the inequities in the healthcare system, allowing biased technology to resolve issues concerning an individual's health. Black people are more susceptible to organ failure and require immediate medical attention, but many hospitals are using algorithms that place Black patients lower on the transplant list than White patients.¹²⁸ Another algorithm used by hospitals to predict patients needing follow-up care disproportionately favored White patients where there should have been an even split.¹²⁹

Obtaining financial security, economic freedom, and generational wealth is a challenge for African Americans because of racist banking practices. Designed to reduce biases inherent in face-to-face communication with banks, the user data generated to create these algorithms and the lack of diversity in the financial sector have only magnified the biases Black and Hispanic people encounter in receiving objective credit decisions. Algorithms incorporate biases that can reduce an individual's ability to access new credit cards, raise their credit lines, get approved for loans, or qualify for lower interest rates.¹³⁰ Systems are often not in sync with the ebbs and flows of market conditions, especially in dealing

¹²² *An Overview of the First Step Act*, FED. BUREAU PRISONS, <https://www.bop.gov/inmates/fsa/overview.jsp> (last visited Dec. 30, 2022).

¹²³ Carrie Johnson, *Flaws Plague a Tool Meant to Help Low-Risk Federal Prisoners Win Early Release*, NAT'L PUBLIC RADIO (Jan. 26, 2022, 5:00 AM), <https://www.npr.org/2022/01/26/1075509175/justice-department-algorithm-first-step-act>.

¹²⁴ *Id.*

¹²⁵ *Id.*

¹²⁶ Duncan Purves & Jeremy Davis, *Criminal Justice Algorithms: Being Race-Neutral Doesn't Mean Race-Blind*, THE CONVERSATION (Mar. 31, 2022, 8:44 AM), <https://theconversation.com/criminal-justice-algorithms-being-race-neutral-doesnt-mean-race-blind-177120>.

¹²⁷ *Id.*

¹²⁸ Rae Ellen Bichell & Cara Anthony, *For Black Kidney Patients, An Algorithm May Help Perpetuate Harmful Racial Disparities*, WASH. POST (June 6, 2021, 8:00 AM), https://www.washingtonpost.com/health/black-kidney-patients-racial-health-disparities/2021/06/04/7752b492-c3a7-11eb-9a8d-f95d7724967c_story.html.

¹²⁹ Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCIENCE 447, 448 (2019).

¹³⁰ *Banking on the Bots: Unintended Bias in AI*, DELOITTE, <https://www2.deloitte.com/uk/en/pages/financial-services/articles/banking-on-the-bots-unintended-bias-in-ai.html> (last visited Dec. 30, 2022).

Should the United States Adopt AI Regulation

with high inflation that force people with low-income jobs to depend on credit more to provide for themselves and their families.

AI has been used to spread political disinformation and stymie student protests at many colleges.¹³¹ With campaign funds increasingly going towards digital ad spending, false information is spread online about police presence at polling places or incorrect information about time, place, and manner of voting intending to prevent racial minorities from exercising their constitutional right.¹³² Some of these practices include telling people to vote via text, informing voters a birth certificate or naturalization document is required to register, and telling voters to boycott the election.¹³³ Many college police departments use Social Sentinel, an AI tool intended to detect threatening tweets about campus, to mitigate protest by monitoring what students say on social media.¹³⁴ Considering the protest that occurred in 2020 following the death of George Floyd and the resulting political awakening among Gen-Z students, allowing campus police to use this tool could result in students of color being disproportionately detained for exercising their freedom of speech and right to privacy.

We use facial recognition technology to unlock smartphones and access our banking information or health records. State and local law enforcement agencies also use facial recognition technology to identify suspects. The technology has falsely identified African American and Asian faces more than Caucasian faces, it had more difficulty identifying women than men, and it falsely identified older adults up to 10 times more than middle-aged adults.¹³⁵ These are only a few examples of how AI-based decision-making has magnified pre-existing biases and possibly created new biases. Since AI relies on user-generated content or data collection systems, they incorporate biases and reproduce inequalities we commonly see in face-to-face interactions. In doing so, these tools are following existing societal norms by favoring aspects of human behavior that are easily quantifiable over those which are hard to measure.¹³⁶

¹³¹ Molly Cohen, *Several Colleges have Used an Artificial Intelligence Tool to Track Student Protests*, DAILY PENNSYLVANIAN (Sept. 26, 2022, 11:44 PM), <https://www.thedp.com/article/2022/09/ai-monitoring-student-protests-social-sentinel>; Young Mie Kim, *Voter Suppression Has Gone Digital*, BRENNAN CTR. FOR JUS. (Nov. 20, 2018), <https://www.brennancenter.org/our-work/analysis-opinion/voter-suppression-has-gone-digital>.

¹³² Kim, *supra* note 131.

¹³³ *Id.*

¹³⁴ Arijit Douglas Sen & Derëka Bennett, *Tracked: How Colleges Use AI To Monitor Student Protests*, PULITZER CTR. (Sept. 20, 2022), <https://pulitzercenter.org/stories/tracked-how-colleges-use-ai-monitor-student-protests>.

¹³⁵ Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>.

¹³⁶ Ntoutsis Et Al., *Bias in Data-Driven Artificial Intelligence Systems—An Introductory Survey*, WILEY PERIODICALS, Feb. 2020.

V. Proposal

A. Amendments to the National Artificial Intelligence Initiative Act

Similar to the way the EU AI Act integrates preexisting EU fundamental rights legislation, the NAIIA should include an AI Bill of Rights. The founding fathers authored the Bill of Rights to control the actions of the State and Federal governments. Some of the rights define the rights of the people, and others serve as restraints on governmental power. As AI and facial recognition technology become part of daily life, Americans are aware of the privacy harms that occur in how these systems collect our data and use it in a manner that unlawfully encroaches upon our fundamental rights. An AI Bill of Rights is a reasonable starting point to preserve individual rights and government restraint.

In reaching this goal, the White House Office of Science and Technology Policy (“OSTP”) released its blueprint for protecting civil rights when using artificial intelligence (the “Blueprint”).¹³⁷ The Blueprint identified five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence.¹³⁸ The five principles include protection from unsafe or ineffective systems, algorithms and systems should be used and designed to prevent discrimination, protection from abusive data practices via built-in protections allowing the user to have agency over their data, notice that an automated system is being used and understanding how it contributes to outcomes that impact the user, and the ability to opt-out of the automated system and have access to a person who can remedy problems the user encounters.¹³⁹

The first principle emphasizes the need for diverse communities to be involved in the development of automated systems to identify concerns, risks, and potential impacts.¹⁴⁰ Since automated systems often rely on historical data that include potentially biased information, they should be designed to protect individuals from inappropriate data use.¹⁴¹ The second principle calls for proactive measures to protect individuals and communities from algorithmic discrimination.¹⁴² These protections include proactive equity assessments as part of the design phase, use of data to ensure accessibility for people with disabilities, disparity assessments and mitigation.¹⁴³ The third principle supports limiting data collection to the user’s reasonable expectations and that only data strictly necessary for the specific context is collected.¹⁴⁴ The user should be protected via built-in privacy

¹³⁷ See OFF. OF SCIENCE & TECH. POL’Y, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE 2 (2022).

¹³⁸ *Id.* at 3.

¹³⁹ *Id.* at 5-7.

¹⁴⁰ OFF. OF SCIENCE & TECH. POL’Y, *supra* note 137, at 15.

¹⁴¹ *Id.*

¹⁴² OFF. OF SCIENCE & TECH. POL’Y, *supra* note 137, at 23.

¹⁴³ *Id.*

¹⁴⁴ OFF. OF SCIENCE & TECH. POL’Y, *supra* note 137, at 30.

Should the United States Adopt AI Regulation

protections, data minimization, use and collection limitations, and transparency.¹⁴⁵ Users should control access to and use of their data, and consent to data collection should only be given when necessary.¹⁴⁶ The fourth principle focuses on how automated systems should provide notice of use and explanations as to how and why a decision was made or an action was taken by the system.¹⁴⁷ These systems should include clear descriptions of the overall system functioning, the individual or organization responsible for the system, and explanations of outcomes that are clear, timely, and accessible.¹⁴⁸ The fifth principle stresses the importance of human intervention to determine whether it is appropriate for a user to opt out from automated systems in favor of a human alternative.¹⁴⁹ Users should have access to timely human consideration and remedy by a fallback process if an automated system fails or it produces an error.¹⁵⁰

The Blueprint serves as a stepping stone for protecting the rights, liberties, and privacy of the American public in the age of artificial intelligence. However, it does not address the role of government agencies in designing, using, and deploying AI systems.¹⁵¹ As mentioned earlier, some of the most consequential outcomes of using AI systems come from law enforcement and government agencies. A second task force should be committed to government oversight and accountability.¹⁵² An AI Bill of Rights should restrain the government's role as both a deployer of AI and a recipient of AI-generated data.¹⁵³ A federal task force combined with legislation passed by cities banning government and private sector use of facial recognition technology would aid in mitigating potential ethical harms of AI in our federalist society.¹⁵⁴

B. Expanded Role for the National Artificial Intelligence Advisory Committee

In addition to the NAIAC's duties to the President, the committee should take measures to ensure fair and responsible use of AI while acknowledging the biases in these technologies. There are currently no federal laws that address issues concerning biased algorithms that allow renters to prey on minorities, voter intimidation laws do not address online disinformation, and individuals cannot sue tech companies for predatory practices.¹⁵⁵ Providing activists with

¹⁴⁵ *Id.*

¹⁴⁶ *Id.*

¹⁴⁷ OFF. OF SCIENCE & TECH. POL'Y, *supra* note 137, at 40.

¹⁴⁸ *Id.*

¹⁴⁹ OFF. OF SCIENCE & TECH. POL'Y, *supra* note 137, at 46.

¹⁵⁰ *Id.*

¹⁵¹ Donna Etemadi, *AI Bill of Rights Must Protect Against Government Overreach*, LAW360 (Oct. 27, 2022, 2:16 PM), <https://www.law360.com/articles/1542989/ai-bill-of-rights-must-protect-against-government-overreach>.

¹⁵² *Id.*

¹⁵³ *Id.*

¹⁵⁴ Tom Simonite, *Portland's Face-Recognition Ban Is a New Twist on 'Smart Cities'*, WIRED (Sept. 21, 2020, 9:00 AM), <https://www.wired.com/story/portlands-face-recognition-ban-twist-smart-cities/>.

¹⁵⁵ *Id.*

Should the United States Adopt AI Regulation

a place to speak could help in passing legislation that limits harmful uses of AI. Similar to the EU AI Act, the NAIAC could employ degrees of high, minimal, and no risk AI systems to determine appropriate levels of regulation.¹⁵⁶ This would allow the NAIAC to recommend more stringent regulatory actions on the use of AI in financial services, healthcare, employment, and criminal justice.¹⁵⁷

The NAIAC could recommend that the NAIIO place additional systems that monitor for potential bias issues once an AI system is in public use.¹⁵⁸ Provide feedback channels that allow users to report errors to a human instead of an AI system.¹⁵⁹ Ensure some policies and procedures address critical functions throughout the AI lifecycle so that results are repeatable and potential risks are recorded.¹⁶⁰ Require AI providers to submit documentation on how their bias management processes are implemented and recorded at each stage.¹⁶¹ Establish a subcommittee that is responsible for monitoring accountability mechanisms involved in the training and deployment of AI systems.¹⁶² Require that providers of high risk systems have effective risk mitigation procedures in place that allow them to quickly detect potential biases and allocate more resources to respond to risks that are most likely to cause real-world harm.¹⁶³

The NAIAC could establish conformity assessments and post-market monitoring systems providers must undergo before placing the system on the market. Unlike the EU AI Act, the NAIAC should establish separate conformity assessment structures for systems governed by existing product safety legislation so that these products satisfy the NAIIA.¹⁶⁴ The conformity assessment should be like the EU AI Act's requirements for "stand-alone" systems, which requires providers to conduct their own conformity assessment and submit it for review.¹⁶⁵ The post-market monitoring systems should establish procedures for how high-risk AI systems are designed and deployed and how to implement and maintain post-market monitoring of the respective high-risk system.¹⁶⁶

V. Conclusion

Artificial intelligence is changing the world for the better by creating new jobs, transforming health care, preventing financial fraud, and making more resources available to significant numbers of peoples. As a result, governments such as

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

¹⁵⁸ Reva Schwartz et al., *Towards A Standard for Identifying and Managing Bias in Artificial Intelligence*, NAT'L INST. OF STANDARDS & TECH., at 42 (Mar. 2022), <https://nvlpubs.nist.gov/nistpubs/Special-Publications/NIST.SP.1270.pdf>.

¹⁵⁹ *Id.* at 43.

¹⁶⁰ *Id.*

¹⁶¹ *Id.* at 44.

¹⁶² *Id.* at 45.

¹⁶³ *Id.* at 46.

¹⁶⁴ EU AI Act, *supra* note 1, at ¶ 1.2.

¹⁶⁵ *Id.* at ¶ 5.2.

¹⁶⁶ Mökander, *supra* note 69, at 252.

Should the United States Adopt AI Regulation

the United States and the European Union have passed legislation to maximize these benefits. Where American AI legislation has focused more on establishing U.S. leadership in AI research and development, the European Union has taken a more ethical approach by prioritizing efforts that mitigate risks. The European Union strives to protect fundamental rights by using trustworthy AI that preserves privacy. The E.U. AI Act is imperfect and could do more to provide a robust enforcement mechanism for high-risk uses of AI. The first step, which the European Union has done, is to acknowledge the risks associated with AI and data-driven technologies and establish risk prevention or mitigation measures that address these issues.

In contrast, the United States has placed the ethical governance of AI in the hands of local governments and the private sector. Only some people are in unison on how to regulate AI. Only a small percentage of cities and companies have been proactive about imposing restrictions. Under this laissez-faire approach to AI regulation, people of color are at a greater risk of exploitation and benefit less from using the current AI systems. As grim as it may seem, there is an opportunity for the United States to preserve the free market and protect fundamental rights. Some systems allow government oversight and accountability for how AI systems are used and designed, how data is collected, and what data is collected. It is critical that the United States also strives to protect fundamental rights by putting into public use trustworthy AI that preserves privacy and truly benefits every American.