

10-31-2023

The Ideal Approach to Artificial Intelligence Legislation: A Combination of the United States and European Union

Dane Chapman
University of Miami School of Law.

Follow this and additional works at: <https://repository.law.miami.edu/umlr>



Part of the [International Law Commons](#), [Law and Politics Commons](#), [Law and Society Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Dane Chapman, *The Ideal Approach to Artificial Intelligence Legislation: A Combination of the United States and European Union*, 78 U. MIA L. Rev. 265 (2023)

Available at: <https://repository.law.miami.edu/umlr/vol78/iss1/8>

This Note is brought to you for free and open access by the Journals at University of Miami School of Law Institutional Repository. It has been accepted for inclusion in University of Miami Law Review by an authorized editor of University of Miami School of Law Institutional Repository. For more information, please contact mperezm@law.miami.edu, library@law.miami.edu.

The Ideal Approach to Artificial Intelligence Legislation: A Combination of the United States and European Union

DANE CHAPMAN*

The evolution of Artificial Intelligence (“A.I.”) from a speculative concept depicted in science fiction to its integration into various aspects of everyday life has brought about complex challenges for contemporary legislators. The proliferation of A.I. technology has led to a growing recognition of the need for regulation, as it poses both promises and threats to society. On the one hand, A.I. has the potential to enhance efficiency in various fields, such as medicine and automation of routine tasks. On the other hand, if left unregulated, A.I. has the potential to undermine democratic principles and infringe upon fundamental rights. Thus, legislators are facing the delicate task of balancing regulation with the need to foster continued innovation in the field of A.I. Both the United States (“U.S.”) and the European Union (“E.U.”) have begun taking steps towards the development of A.I. legislation, recognizing the need for a comprehensive approach to address the multifaceted challenges posed by this rapidly advancing technology.

* Digital Editor, *University of Miami Law Review*, Volume 78; J.D. Candidate 2024, University of Miami School of Law; B.A. 2020, Florida Atlantic University. Thank you to my colleagues at the *University of Miami Law Review* for their assistance in editing this publication. Thank you to my faculty advisor, Professor Marcia Narine Weldon, for her guidance and input throughout the drafting stages. Finally, thank you to my friends and family for their endless encouragement and support.

INTRODUCTION	266
I. BACKGROUND OF A.I.	268
A. <i>A.I.'s Current Uses</i>	268
B. <i>Threats of A.I.</i>	270
II. LEGISLATIVE REMEDIES IN THE U.S. AND E.U.	272
A. <i>A.I. Regulation in the U.S.</i>	273
1. A.I. BILL OF RIGHTS	274
2. ALGORITHMIC ACCOUNTABILITY ACT OF 2022	278
B. <i>A.I. Regulation in the E.U.</i>	281
1. EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT	282
III. CURRENT AND FUTURE IMPLICATIONS OF U.S. AND E.U.	
A.I. LEGISLATION	287
A. <i>What Is the Ideal Approach? Fragmentation or</i> <i>Centralization?</i>	287
B. <i>The Ideal Approach: A Combination of the U.S. and</i> <i>E.U.</i>	290
CONCLUSION	295

INTRODUCTION

As the lines between human and machine blur, the race to harness the power of A.I. heats up, raising questions of what it truly means to be alive. A.I. is a general term encompassing technologies that can autonomously learn and respond to their environments.¹ Such technologies include machine learning, robotic process automation, language processing, and networks.² Research and development into A.I. officially began in the 1950s when Alan Turing, the “father of computer science,” created the “Turing Test” to determine if machines were A.I.³

A.I. is a broad field that encompasses two distinct categories: (1) narrow or weak A.I. and (2) general or strong A.I.⁴ Narrow A.I. is

¹ Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106, 114–15 (2019).

² *Id.*

³ *What is Artificial Intelligence (AI)?*, IBM, <https://www.ibm.com/cloud/learn/what-is-artificial-intelligence> (last visited Aug. 15, 2023).

⁴ *Id.*

designed to perform specific tasks like Apple's Siri or Tesla's autonomous vehicles.⁵ General A.I. is a type of A.I. that can perform any intellectual task that a human could.⁶ Despite being a highly sought after goal in the field of A.I., the creation of general A.I. has yet to be achieved, but it serves as the yardstick against which the capabilities of A.I. systems are gauged.⁷

The capabilities of A.I. have also created the need for regulatory oversight to ensure fundamental rights and privileges are not violated.⁸ The U.S. and E.U. have begun drafting legislation to address the threats that unregulated A.I. poses to humans while attempting to allow continued controlled development of A.I.⁹ Scholars and critics have discussed the implications of the U.S. and E.U.'s approaches to this new area of regulation.¹⁰ The underlying approach to A.I. regulation is critical to ensuring the regulation is effective and protects fundamental principles that encompass these democratic institutions. Hence, there is a pressing need for a well-thought-out approach that balances the potential risks and benefits of A.I. development, ensuring that the rights and freedoms of individuals are not violated in the process.

Part I of this Note discusses the history and origins of A.I., including its present-day applications and the perils it poses. Part II of this Note will then discuss the benefits and drawbacks of the E.U.'s centralized approach to A.I. legislation and the U.S.'s fragmented approach to A.I. legislation. Part III of this Note examines specific pieces of the U.S. and E.U.'s approaches to A.I. regulation and scrutinizes the implications of the proposed legislation. Part III also proposes an optimal regulation model that amalgamates the best features of both the U.S. and E.U. approaches. Part IV concludes by

⁵ *Id.*

⁶ *Id.*

⁷ Manheim & Kaplan, *supra* note 1, at 115 (explaining that passing the Turing Test would mean that a human could not distinguish between an A.I.-generated natural language response and a human in a blind conversation). Futurist Ray Kurzweil has "predicted successful passing of the Turing Test in 2029." *Id.* Thus, strong A.I. remains theoretical, and narrow A.I. is the only topic of conversation for regulation. *See id.*

⁸ *See* discussion *infra* Section I.B.

⁹ *See* discussion *infra* Part II.

¹⁰ *See* discussion *infra* Part III.

offering perspectives for future A.I. regulations that synthesize elements from the U.S. and E.U. approaches.

I. BACKGROUND OF A.I.

A. *A.I.'s Current Uses*

Today, A.I. is regularly used in speech recognition software like Amazon's Alexa, in customer service tools like virtual agents on e-commerce sites, computer vision like autonomous driving, recommendation engines like personalized advertisements based on a user's search history, and the stock market like helping an investor make faster trades.¹¹ Further, A.I. is completely revolutionizing healthcare, corporate governance, and education by automating tasks, improving efficiency, and changing the way we learn.¹² However, continued innovation and advancement of A.I. raise significant ethical and societal concerns that threaten our democratic values. Famous A.I. enthusiasts such as Elon Musk,¹³ Stephen Hawking, and researchers at Oxford and UC Berkley acknowledge A.I.'s potential yet warn that A.I. may be humanity's downfall.¹⁴

A.I. has unparalleled potential and power to the point that many fear the amount of industry disruption it could bring. For example, A.I. is used in finance to help make investment decisions and analyze financial data.¹⁵ Betterment, a financial investment company, uses A.I. algorithms to “automate tax loss harvesting, trading, transactions and portfolio management”—all tasks that used to require a

¹¹ See Manheim & Kaplan, *supra* note 1, at 115–16.

¹² Crispin Coombs et al., *The Strategic Impacts of Intelligent Automation for Knowledge and Service Work: An Interdisciplinary Review*, J. STRATEGIC INFO. SYS., Mar. 9, 2020, at 1, <https://doi.org/10.1016/j.jsis.2020.101600>.

¹³ Steve Mollman, *Elon Musk's History with OpenAI—the Maker of A.I. Chatbot ChatGPT—as Told by ChatGPT Itself*, FORTUNE (Dec. 11, 2022, 8:10 PM), <https://fortune.com/2022/12/11/elon-musk-history-with-chatgpt-maker-openai-as-told-by-the-ai-chatbot-itself>.

¹⁴ Kelsey Piper, *Why Elon Musk Fears Artificial Intelligence*, VOX (Nov. 2, 2018, 12:10 PM), <https://www.vox.com/future-perfect/2018/11/2/18053418/elon-musk-artificial-intelligence-google-deepmind-openai>.

¹⁵ Sam Daley, *36 Artificial Intelligence Examples Shaking Up Business Across Industries*, BUILT IN (Feb. 17, 2023), <https://builtin.com/artificial-intelligence/examples-ai-in-industry>.

lot of human elbow grease and know-how.¹⁶ Other notable applications of A.I. are virtual assistants, self-driving cars, healthcare, manufacturing, and customer service.¹⁷

One of the most popular forms of customer service A.I. is ChatGPT. ChatGPT, created by Open AI, is an A.I.-powered chatbot that acts as a virtual assistant using natural language processing.¹⁸ This powerful virtual assistant is powered by the “Generative Pre-trained Transformer 4,” which is a language processing software that enables it to provide detailed answers to virtually any question that one asks it.¹⁹ ChatGPT has shown tremendous promise in the customer service, education, personal assistant, and training industries.²⁰ For example, ChatGPT has passed a practice bar exam, written computer code, and summarized legal documents in the blink of an eye.²¹ Notably, ChatGPT has already been used for illegitimate purposes, such as cheating in school²² and hacking by cybercriminals.²³ These concerns about this new A.I. technology have only raised more calls for additional legislation and regulation.²⁴

ChatGPT is the first publicly available fully functioning A.I. with the capability of answering almost any question with a coherent, unique response, previously only fantasized in science fiction

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ John Bailey, *Meet ChatGPT: The AI Chatbot that Can Write Code, Pass Exams, and Generate Business Ideas*, AEI (Dec. 16, 2022), <https://www.aei.org/technology-and-innovation/meet-chatgpt-the-ai-chatbot-that-can-write-code-pass-exams-and-generate-business-ideas>.

¹⁹ *See id.*

²⁰ *Id.*

²¹ *Id.*

²² Rashi Shrivastava, *Teachers Fear ChatGPT Will Make Cheating Easier than Ever*, FORBES (Dec. 12, 2022, 1:11 PM), <https://www.forbes.com/sites/rashishrivastava/2022/12/12/teachers-fear-chatgpt-will-make-cheating-easier-than-ever>.

²³ Crane Hassold, *The Double-Edged Sword of ChatGPT: How Threat Actors Could Use It for Evil*, ABNORMAL (Dec. 12, 2022), <https://abnormalsecurity.com/blog/double-edged-sword-of-chatgpt>.

²⁴ David Hickton, *ChatGPT Could Transform Society – and Its Risks Require Quick Regulation*, THE HILL (Jan. 19, 2023, 9:00 AM), <https://thehill.com/opinion/technology/3812597-chatgpt-could-transform-society-and-its-risks-require-quick-regulation>.

movies.²⁵ ChatGPT is completely different from past A.I. chat programs because of its ability to respond using human-like language.²⁶ In other words, you would not be able to tell an A.I. program was answering the question.²⁷ Moreover, ChatGPT does not just reply with pre-programmed responses; rather, it internalizes the question against the data set it was trained on and formulates a completely unique response.²⁸ The ease of accessibility and limitless potential of this program highlight the importance of robust regulation to mitigate the potential dangers associated with such power.²⁹ ChatGPT also publicly signifies a shift away from an information era to a knowledge era, whereby knowing how to use tools like ChatGPT can feign intelligence on subjects that people spend years studying.³⁰

B. *Threats of A.I.*

The right to privacy, self-autonomy, and equal protection are fundamental principles underlying contemporary democratic institutions.³¹ Unregulated A.I. threatens these principles—algorithms and programs can now track and collect data on every aspect of people’s lives, leading to a loss of trust and control of democratic institutions.³² The most significant threats of A.I. are bias and control.³³ As shown below, these threats are now well documented, highlighting the need for adequate regulation and legislation.

²⁵ Luke Hurst, *ChatGPT: Why the Human-like AI Chatbot Suddenly Has Everyone Talking*, EURONEWS (Dec. 15, 2022), <https://www.euronews.com/next/2022/12/14/chatgpt-why-the-human-like-ai-chatbot-suddenly-got-everyone-talking>.

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ *See id.*

³¹ *See generally* Manheim & Kaplan, *supra* note 1, at 116–52.

³² Dirk Helbing et al., *Will Democracy Survive Big Data and Artificial Intelligence?*, SCI. AM. (Feb. 25, 2017), <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/> (discussing that continued, unregulated development of A.I. may lead to inadequate “transparency and democratic control” going forward).

³³ *See* Nithesh Naik et al., *Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?*, FRONTIERS SURGERY, Mar. 14, 2022, at 2, <https://doi.org/10.3389/fsurg.2022.862322>.

Left unchecked, A.I. results in unintentional bias and privacy violations in numerous industries.³⁴ The reasons why these violations occur are often complex and challenging to understand. Some scholars and studies argue that this discrimination occurs because of the data on which A.I. is programmed, or because it encounters a new scenario and reacts differently.³⁵

For example, Amazon's use of an A.I. algorithm in the hiring process filtered out women's resumes and people who graduated from two all-women's colleges.³⁶ Because these algorithms make decisions based only on the data with which they are programmed, it is paramount to ensure the data or the programmer is neutral.³⁷ Amazon's algorithm exemplifies the limitations of machine learning regarding the unpredictability it entails when encountering new environments and the threats unregulated A.I. poses.³⁸

Additionally, even popular children's toys, like Barbie, now have A.I. incorporated into the doll.³⁹ The famous doll can now collect data and respond to its environment, sparking a new discussion about the sensitive information it collects and the influence it has on children.⁴⁰ Researcher Matt Jakubowski reported that he could easily hack into the Barbie doll and collect the information she had

³⁴ See, e.g., Manheim & Kaplan, *supra* note 1, at 121 (discussing that unregulated A.I. in the health industry collecting data on people could "disqualify candidates for lower insurance premiums").

³⁵ See Araz Tacihagh, *Governance of Artificial Intelligence*, 40 POL'Y & SOC'Y 137, 140 (2021), <https://doi.org/10.1080/14494035.2021.1928377> ("A major challenge faced by most AI applications to date stems from their lack of generalizability to different contexts, in which they can face unexpected situations widely referred to as 'corner cases' that the system had not been trained to handle."); see also *id.* at 141 ("As [machine learning] algorithms can learn from data gathered from society to make decisions, they could not only conflict with the original ethical rules they were programmed with but also reproduce the inequality and discriminatory patterns of society that is contained in such data.").

³⁶ Jonathan Shaw, *Artificial Intelligence and Ethics*, HARV. MAG. (Jan.–Feb. 2019), <https://www.harvardmagazine.com/2019/01/artificial-intelligence-limitations>.

³⁷ See *id.*

³⁸ See *id.*

³⁹ Whitney Meers, *Hello Barbie, Goodbye Privacy? Hacker Raises Security Concerns*, HUFFPOST (Nov. 30, 2015, 4:45 PM), https://www.huffpost.com/entry/hello-barbie-security-concerns_n_565c4921e4b072e9d1c24d22.

⁴⁰ *Id.*

gathered.⁴¹ Barbie's lack of security and the amount of information she collects undeniably raises the questions of where the data in the dolls are stored, what protections or regulations are in place, and how easy it is to access the data.

A.I. programs can autonomously collect our data, track our movements, and peer into almost every aspect of our lives with virtually no regulation.⁴² This unfettered access over our information and data violates fundamental democratic principles.⁴³ As this technology continues to develop, A.I.'s ability to collect information will improve; and without proper regulation, our fundamental privacy interests will be completely eroded.⁴⁴

II. LEGISLATIVE REMEDIES IN THE U.S. AND E.U.

A.I.'s continued expansion and development has undeniably motivated legislative bodies to act. However, the U.S. and the E.U. have differing approaches to regulating A.I. For example, there is no comprehensive federal legislation specifically targeting A.I. in the U.S.⁴⁵ Instead, A.I. is regulated through an amalgamation of federal laws and regulations that apply to specific industries or activities,⁴⁶ which is known as a "fragmented approach" to A.I. regulation.⁴⁷ All of the proposed pieces of legislation in the U.S. take a similar fragmented approach to regulating A.I.⁴⁸

⁴¹ *Id.*

⁴² *See* Manheim & Kaplan, *supra* note 1, at 108–10.

⁴³ *Id.* at 110.

⁴⁴ *Id.* at 129–30.

⁴⁵ *See* Daniel J. Felz et al., *Privacy, Cyber & Data Strategy Advisory: AI Regulation in the U.S.: What's Coming, and What Companies Need to Do in 2023*, ALSTON & BIRD (Dec. 9, 2022), <https://www.alston.com/en/insights/publications/2022/12/ai-regulation-in-the-us>.

⁴⁶ *See id.*

⁴⁷ PETER CIHON ET AL., SHOULD ARTIFICIAL INTELLIGENCE GOVERNANCE BE CENTRALISED? SIX DESIGN LESSONS FROM HISTORY § 1 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3761636 (defining "fragmentation or decentralization" as a "patchwork of international organisations and institutions which focus on a particular issue area [like A.I.] but differ in scope, membership and often rules"). An example of this is the multitude of different international environmental agreements and treaties. *Id.*

⁴⁸ *See* discussion *infra* Section II.A.

Conversely, the E.U. takes a “centralized approach” to regulation and is attempting to create the first piece of horizontal A.I. legislation.⁴⁹ The E.U. is currently in the process of adopting a proposed comprehensive set of rules and regulations targeted explicitly at A.I. through the European Union Artificial Intelligence Act.⁵⁰ Both the U.S.’s fragmented approach and the E.U.’s centralized approach to A.I. regulation have advantages and disadvantages. In recent years, the U.S. has taken notable steps toward A.I. regulation.⁵¹

A. *A.I. Regulation in the U.S.*

There is no specific federal legislation regulating A.I. in the U.S.⁵² Instead, a hodgepodge of federal agencies and state governments regulate A.I.⁵³ However, the Biden administration’s recent Blueprint for an A.I. Bill of Rights⁵⁴ and the proposed Algorithmic Accountability Act of 2022⁵⁵ are seen as fundamental steps towards A.I. regulation.

A.I. policy and legislation in the U.S. is centered in the executive branch.⁵⁶ Past, current, and proposed A.I. legislation in the U.S. all

⁴⁹ See discussion *infra* Section II.B. Centralization means that the legislative authority concerning A.I. will be centered in the E.U. itself, not the member states. Interview by Gregory C. Allen with Dragos Tudorache, Member of the Eur. Parliament, Co-rapporteur of the E.U. A.I. Act (Sept. 19, 2022).

⁵⁰ Mauritz Kop, *E.U. Artificial Intelligence Act: The European Approach to AI*, TRANSATLANTIC ANTITRUST AND IPR DEVS., Oct. 1, 2021, at 1, <https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai>.

⁵¹ See discussion *infra* Section II.A.

⁵² See Louis Lehot, Foley & Lardner, *United States: Artificial Intelligence Comparative Guide*, MONDAQ (Dec. 6, 2022), <https://www.mondaq.com/united-states/technology/1059776/artificial-intelligence-comparative-guide> (“Despite AI’s ubiquity across every technology and healthcare field, there is no comprehensive federal legislation on AI in the United States to date.”).

⁵³ See Manheim & Kaplan, *supra* note 1, at 160–62.

⁵⁴ WHITE HOUSE OFF. OF SCI. & TECH. POL’Y, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE 2 (2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.

⁵⁵ Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 1 (2022).

⁵⁶ OLANREWAJU O. AKINOLA ET AL., COMPARATIVE ANALYSIS REGULATORY OF AI AND ALGORITHM IN UK, EU AND USA, § III(C) (2022), <http://dx.doi.org/10.2139/ssrn.4212588>.

have a common theme of being introduced on a sectoral, agency-by-agency basis.⁵⁷ The Trump administration approached A.I. with a “light touch,” and the administration’s regulatory approach to A.I. was contained entirely within the executive branch.⁵⁸ The Trump administration’s approach perpetuated sector-specific A.I. regulation. For example, the Department of Transportation was exclusively involved in regulating autonomous vehicles.⁵⁹ Moreover, the Trump administration’s approach to A.I. regulation and its executive guidance was very hands-off and did not address the risks A.I. poses to human rights.⁶⁰

Recognizing the need to protect privacy interests and democratic values from the continued development of A.I., the Biden administration drafted the Blueprint for the A.I. Bill of Rights,⁶¹ spearheaded by Dr. Alondra Nelson.⁶² Dr. Nelson—Deputy Assistant to the President and OSTP Deputy Director for Science and Society—along with the White House Office of Science and Technology Policy (OSTP), released the A.I. Bill of Rights to further the Biden administration’s vision of developing A.I. while protecting individual rights and democratic principles.⁶³

1. A.I. BILL OF RIGHTS

On October 24, 2022, the Biden administration released the highly anticipated ‘Blueprint’ for an A.I. Bill of Rights (“A.I.BoR”).⁶⁴ The A.I.BoR is a set of ethical principles for A.I. and a crucial step toward recognizing the risks and benefits that A.I. poses.⁶⁵ The A.I.BoR is a detailed exposition of A.I.’s civil rights

⁵⁷ *Id.*

⁵⁸ See Alex Engler, *The AI Bill of Rights Makes Uneven Progress on Algorithmic Protections*, BROOKINGS (Nov. 21, 2022), <https://www.brookings.edu/2022/11/21/the-ai-bill-of-rights-makes-uneven-progress-on-algorithmic-protections>.

⁵⁹ Alex Engler, *New White House Guidance Downplays Important AI Harms*, BROOKINGS (Dec. 8, 2020), <https://www.brookings.edu/blog/techtank/2020/12/08/new-white-house-guidance-downplays-important-ai-harms>.

⁶⁰ See *id.* (“[T]here is a real risk that this document becomes a force for maintaining the status quo, as opposed to addressing serious AI harms.”).

⁶¹ WHITE HOUSE OFF. OF SCI. & TECH. POL’Y, *supra* note 54, at 2.

⁶² *Id.* at 59.

⁶³ *Id.* at 3.

⁶⁴ *Id.* at 2.

⁶⁵ *Id.*

risks and harms, an aspect missing from the Trump administration's approach to A.I. regulation.⁶⁶ Notably, the A.I.BoR recognizes the need for A.I. principles to protect democratic values and “protect civil rights, civil liberties, and privacy.”⁶⁷

The A.I.BoR lays out five core principles aimed at addressing A.I. risks. First, the A.I. must be safe and effective due to continued concerns of A.I. not functioning as intended and A.I. being dangerous.⁶⁸ Second is “Algorithmic Discrimination Protections,” ensuring that people are not discriminated against by A.I. based on their mutable or immutable characteristics.⁶⁹ Third, the “Data Privacy” principle helps to prevent the unrestricted use and collection of data.⁷⁰ Fourth, the “Notice and Explanation” principle encourages transparency in companies that use A.I. to make decisions so that the customer knows what role the A.I. is playing in any decision-making processes.⁷¹ Fifth, the “Human Alternatives, Consideration, and Fallback” principle encourages the ability to appeal the decision and opt out of A.I. making the final decision in specific contexts.⁷² These guidelines are very similar to the framework published by the E.U. in 2019, which is currently being used in the E.U. A.I. Act.⁷³

The broad nature of the A.I.BoR comes with a few significant advantages over other proposed legislation. The A.I.BoR endorses agency-led and sector-specific applications to enforce its principles.⁷⁴ It avoids defining A.I.—one of the contentious debates in the

⁶⁶ *See id.*

⁶⁷ WHITE HOUSE OFF. OF SCI. & TECH. POL'Y, *supra* note 54, at 4.

⁶⁸ *Id.* at 5.

⁶⁹ *Id.*

⁷⁰ *Id.* at 6.

⁷¹ *Id.*

⁷² *Id.* at 7 (discussing how people should be able to opt out from automated systems making the final decision in certain contexts as long as a human alternative is available).

⁷³ Natasha G. Kohne et al., *White House Reveals Long-Anticipated 'AI Bill of Rights,'* AKIN (Oct. 21, 2022), <https://www.akingump.com/en/news-insights/white-house-reveals-long-anticipated-ai-bill-of-rights.html>.

⁷⁴ *See* Engler, *supra* note 58; *see also* WHITE HOUSE OFF. OF SCI. & TECH. POL'Y, *supra* note 54, at 5 (“Systems should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards.”) (emphasis added)).

E.U. A.I. Act—and leaves it up to the individual agency to make the determination.⁷⁵ The advantages of this application-specific A.I. regulatory guidance allow for more accessible applications because some of the work for A.I. has already begun years before and will result in more specific definitions, leading to more effective regulation.⁷⁶

Additionally, the A.I.BoR will motivate agencies to address sector-specific A.I. regulations and collaborate with stakeholders.⁷⁷ Because of sector-specific A.I. governance, agencies are more likely to be able to increase their employment capacity to handle distributed A.I. governance.⁷⁸ The A.I.BoR avoids generalized definitions of A.I. and does not have a list of rules that must apply to all A.I. applications and algorithms.⁷⁹ The lack of broad, generalized definitions enables agencies to define algorithms in specific circumstances, allowing them to create more narrow guidance for A.I. applications.⁸⁰

In the same vein, many of these sector-specific advantages also present disadvantages. Firstly, the A.I.BoR does not actually require agencies to take any action or abide by any principle outlined in the Blueprint, as its principles are non-binding.⁸¹ The A.I.BoR also does

⁷⁵ Matt O’Shaughnessy, *One of the Biggest Problems in Regulating AI Is Agreeing on a Definition*, CARNEGIE ENDOWMENT FOR INT’L PEACE (Oct. 6, 2022), <https://carnegieendowment.org/2022/10/06/one-of-biggest-problems-in-regulating-ai-is-agreeing-on-definition-pub-88100>.

⁷⁶ See Leuven Centre for Global Governance Studies, *Transatlantic Lecture: E.U. and U.S. Approaches to Regulating Artificial Intelligence: The U.S. Approach*, YOUTUBE (Nov. 10, 2022), https://www.youtube.com/watch?v=7YZO_MJKR_QM. Certain agencies in the U.S. already have A.I. regulations and policies in place, like the Department of Transportation on autonomous cars and Human Health Services on A.I. in medical devices. *Id.*

⁷⁷ See Engler, *supra* note 58. For example, the Property Appraisal and Valuation Equity (PAVE) action plan was created by the Department of Housing and Urban Development (HUD) when it was pressured by advocacy groups, like the Fair Housing Group. Thus, HUD enacted the PAVE action plan to address “regulation on automated valuation models, which is a type of AI system known to produce larger appraisal and valuation errors in predominantly Black neighborhoods.” *Id.*

⁷⁸ *Id.*

⁷⁹ See *id.*

⁸⁰ See *id.*

⁸¹ See Sharon Goldman, *3 Things the AI Bill of Rights Does (and 3 Things It Doesn’t)*, VENTUREBEAT (Oct. 7, 2022, 9:58 AM), <https://venturebeat.com/ai/3->

not create a change in the law or authority.⁸² The A.I.BoR encourages but does not require agencies to act on these principles.⁸³ Thus, if an agency already does not have the legal ability, capacity, or resources to act on these principles, the A.I.BoR does nothing for them.⁸⁴ Moreover, the A.I.BoR does not cover critical A.I. industries that existing agencies were not already addressing.⁸⁵ Most notably, the A.I.BoR does not address federal law enforcement or require them to take action toward A.I. facial recognition software.⁸⁶ If federal law enforcement agencies do not want to set standards for A.I. facial recognition, they do not have to.⁸⁷ Even worse, in response to the A.I.BoR, many agencies did not respond or provided contradictory answers.⁸⁸

While the A.I.BoR appears promising, it leaves much to be desired. Critics of the A.I.BoR argue that the Biden administration should have given it a more concrete structure and framework to address the issues it left open.⁸⁹ However, the Biden administration drafted the A.I.BoR with politics in mind. A.I. legislation necessarily restricts technology development, an outcome Republicans

things-the-ai-bill-of-rights-does-and-3-things-it-doesnt; *see also* Engler, *supra* note 58.

⁸² Goldman, *supra* note 81; *see also* Engler, *supra* note 58.

⁸³ Goldman, *supra* note 81.

⁸⁴ *See* Engler, *supra* note 58; *see also* Nikki Howell et al., *New EEOC Initiative Targeting AI Technology Used in Hiring Process Presents Increased Risk of Class Litigation*, FOX ROTHSCHILD LLP (June 13, 2022), <https://www.foxrothschild.com/publications/new-eeoc-initiative-targeting-ai-technology-used-in-hiring-process-presents-increased-risk-of-class-litigation>. For example, the Equal Employment Opportunity Commission cannot target the companies that sell A.I. hiring software and can only target the company who purchases the A.I. hiring software. This is a clear lack of legislative authority that the agency has, and the A.I.BoR does not allow them to change any of this. *Id.*

⁸⁵ Goldman, *supra* note 81 (discussing that the A.I.BoR does not address critical sectors such as “educational access, worker surveillance, and . . . law enforcement.”); *see also* Engler, *supra* note 58.

⁸⁶ *See* Engler, *supra* note 58.

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *See generally* Nicol Turner Lee & Jack Malamud, *Opportunities and Blind Spots in the White House’s Blueprint for an AI Bill of Rights*, BROOKINGS (Dec. 19, 2022), <https://www.brookings.edu/blog/techtank/2022/12/19/opportunities-and-blind-spots-in-the-white-houses-blueprint-for-an-ai-bill-of-rights>.

have repeatedly expressed their resentment toward.⁹⁰ The race to technological dominance is a driving factor behind U.S. policymaking, which is why separate legislation restricting technological advancement has a difficult time passing.⁹¹ Thus, policy considerations and politics are why the A.I.BoR had to work with existing law and regulatory roles of agencies.⁹² Additionally, with a split Congress⁹³ and ever-growing competition with China, any legislation that intends to fix any of the disadvantages of the A.I.BoR is unlikely to pass.⁹⁴

2. ALGORITHMIC ACCOUNTABILITY ACT OF 2022

The Algorithmic Accountability Act of 2022 (“AAA”) is a comprehensive piece of proposed legislation on A.I. Initially introduced in 2019, the revised AAA was re-introduced on February 3, 2022.⁹⁵ The AAA requires companies to: (1) consider the potential harms of A.I. that are in high-risk areas through impact assessments and (2) continuously inform the Federal Trade Commission (FTC) and other

⁹⁰ See Leuven Centre for Global Governance Studies, *supra* note 76.

⁹¹ See MIKE MIESEN ET AL., BUILDING A 21ST CENTURY CONGRESS: IMPROVING CONGRESS’S SCIENCE AND TECHNOLOGY EXPERTISE 22 (“Congress has a significant role to play in driving [science and technology] innovation through research and development (R&D) funding: it decides how much to appropriate, what the R&D should focus on, and what organizations will do it.”), <https://www.belfercenter.org/sites/default/files/2019-09/ST/Building21stCenturyCongress.pdf>.

⁹² See Leuven Centre for Global Governance Studies, *supra* note 76.

⁹³ Dennis A. Cardoza et al., *What’s Next in Washington? – January 2023 Edition*, THE NAT’L L. REV. (Jan. 17, 2023), <https://www.natlawreview.com/article/what-s-next-washington-january-2023-edition>.

⁹⁴ See Leuven Centre for Global Governance Studies, *supra* note 76.

⁹⁵ Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 1 (2022); Press Release, Sen. Ron Wyden, Wyden, Booker and Clarke Introduce Algorithmic Accountability Act of 2022 to Require New Transparency and Accountability for Automated Decision Systems (Feb. 3, 2022), <https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems>. The AAA did not receive a vote in a previous session of Congress, but “its provisions could [still] become law by being included in another bill.” *H.R. 6580 (117th): Algorithmic Accountability Act of 2022*, GOVTRACK <https://www.govtrack.us/congress/bills/117/hr6580> (last visited Aug. 15, 2023).

related agencies of the potential harms and risks from the A.I. application.⁹⁶ The AAA substantially expands the FTC’s power by requiring covered companies “to conduct impact assessments for automated decision systems (ADS) and augmented critical decision processes (ACDP) with a significant impact on consumers’ lives.”⁹⁷

Section 2.7 of the AAA defines covered entities as companies with \$50 million in average annual gross receipts, companies with more than \$250 million in equity value, and their subcontractors who use ADS,⁹⁸ which Section 2.1 defines as “systems, software, or processes that use computation to produce outputs to serve as a basis for decision or judgment.”⁹⁹ Lastly, the AAA defines an ACDP as a “process, procedure, or other activity that uses an ADS to arrive at a critical decision.”¹⁰⁰

Critical decision areas include fields such as: “education, employment, essential utilities, family planning, financial services, healthcare, housing, legal services, and other areas deemed critical by the FTC.”¹⁰¹ The impact assessments are routinely reported to the FTC and involve continuous testing and evaluation of the ACDP or ADS about any effects the systems may have on users or stakeholders.¹⁰² Summary reports under the AAA given to the FTC must include a description and category of the critical decision; the intended purpose of the A.I.; identification of stakeholders; testing and evaluation methods (including performance and bias testing); publicly stated limitations on the use of the A.I.; documentation of the data and input information; transparency measures taken; mechanisms for appeal and correction; and the material negative impact the A.I. will have on stakeholders or users.¹⁰³

⁹⁶ H.R. 6580.

⁹⁷ FURKAN GURSOY ET AL., A CRITICAL ASSESSMENT OF THE ALGORITHMIC ACCOUNTABILITY ACT OF 2022 2 (2022), <https://ssrn.com/abstract=4193199>.

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² Kate Kaye, *This Senate Bill Would Force Companies to Audit AI Used for Housing and Loans*, PROTOCOL (Feb. 8, 2022), <https://www.protocol.com/enterprise/revised-algorithmic-accountability-bill-ai>; GURSOY ET AL., *supra* note 97, at 2–3.

¹⁰³ GURSOY ET AL., *supra* note 97, at 2–3.

The framework of the AAA has some notable potential benefits. For example, the bill refrains from using the word “A.I.” and instead uses “ADS,” which effectively avoids defining what A.I. is.¹⁰⁴ The ambiguousness of this definition only cares about whether the ADS is involved in a critical decision process, which helps to “future-proof” the definition.¹⁰⁵ Accordingly, the legislation will likely be much more effective because it will not struggle to classify or define A.I. systems.¹⁰⁶ By focusing on the processes themselves, the bill also avoids becoming outdated the second it is enacted.¹⁰⁷ All users of ADS in critical decision making must document and openly disclose their obligations for transparency and documentation purposes, resulting in better protection for more individuals by solely emphasizing the critical decision processes.¹⁰⁸

The AAA is one of the most comprehensive and well-thought-out pieces of U.S. A.I. legislation proposed to date, and it requires companies to report their programs’ impacts on consumers.¹⁰⁹ Ben Winters, legal counsel at Electronic Privacy Information Center, noted that “it makes the most sense to focus on users rather than vendors.”¹¹⁰ When companies report on their systems’ impact, they will likely do it under different circumstances than a typical consumer or stakeholder, leading to poor and inaccurate results.¹¹¹ In essence, the AAA only requires companies to hold themselves accountable and report the purported risks of their systems. The AAA will create a lot more reporting, which could lead to a greater public repository of A.I. trends and more publicly available information about high-risk A.I., but it lacks enforcement mechanisms.¹¹² Further, the AAA does not provide jurisdiction over any public agen-

¹⁰⁴ Jakob Mökander et al., *The U.S. Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?*, 32 MINDS & MACHS. 751, 753 (2022), <https://doi.org/10.1007/s11023-022-09612-y>.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 752–53.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.* at 752–55.

¹⁰⁹ See Kaye, *supra* note 102.

¹¹⁰ *Id.*

¹¹¹ See *id.*

¹¹² See *id.*

cies, so the FTC would have to pass along the information of a company in violation of an impact assessment to a relevant agency which could then fine or penalize them for violating the impact assessment.¹¹³

The bill is also very unlikely to become law. The core function of the bill is to expand the role of the FTC, which the Republican party already thinks has too much power, and again, it limits technological innovation.¹¹⁴ States are divided on A.I. legislation, with some states passing laws¹¹⁵ while others are pushing back, so there is little hope for this bill passing at a federal level.¹¹⁶

B. *A.I. Regulation in the E.U.*

Conversely, the E.U. has a much more hands-on approach to privacy regulation than the U.S. On May 25, 2018, the E.U. enacted the General Data Protection Regulation (“GDPR”).¹¹⁷ The GDPR is a broad privacy regulation that applies to all member states and associated affiliates¹¹⁸ that are formally within the E.U.¹¹⁹ Unlike the fragmented approach of data regulation in the U.S., the E.U. took a centralized approach to privacy regulation, as the GDPR is an all-encompassing piece of legislation that oversees data collection, use, protection, and sharing laws.¹²⁰ The reasons for the E.U.’s centralization of privacy laws stem from its experience during World War

¹¹³ *See id.*

¹¹⁴ Leuven Centre for Global Governance Studies, *supra* note 76.

¹¹⁵ *See* Danielle Ochs & Jennifer Betts, *California’s Draft Regulations Spotlight Artificial Intelligence Tools’ Potential to Lead to Discrimination Claims*, THE NAT’L L. REV. (May 13, 2022), <https://www.natlawreview.com/article/california-s-draft-regulations-spotlight-artificial-intelligence-tools-potential-to>.

¹¹⁶ *See* Kaye, *supra* note 102. A Washington State bill with similar algorithmic accountability is receiving a lot of pushback from state governments and agencies. *Id.*

¹¹⁷ Ben Wolford, *What is GDPR, the EU’s New Data Protection Law?*, GDPR, <https://gdpr.eu/what-is-gdpr> (last visited Aug. 15, 2023).

¹¹⁸ Manheim & Kaplan, *supra* note 1, at 161–62 (discussing that the GDPR applies to “all entities . . . offering goods or services in the EU, or monitoring people in the EU”).

¹¹⁹ *Id.*

¹²⁰ *See id.*

II, resulting in the need to protect fundamental human rights to ensure a functioning democracy.¹²¹

1. EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT

On April 21, 2021, the European Commission proposed the European Union Artificial Intelligence Act (“E.U. A.I. Act”).¹²² If passed, the Act will be a revolutionary piece of legislation, placing stringent regulations on A.I. while protecting fundamental rights.¹²³ The E.U. A.I. Act is a proposed set of rules and regulations that govern everything from development to the actual use of A.I. within the E.U.¹²⁴ Before the introduction of the E.U. A.I. Act, the E.U. only had “soft laws” that encouraged agencies to enact principles to regulate A.I.¹²⁵ The Act aims to ensure that A.I. is used ethically and responsibly without stifling innovation.¹²⁶ The Act seeks to achieve these principles through centralized, broad rules that will apply horizontally to all E.U. member states.¹²⁷

The E.U. A.I. Act’s primary objective is to protect the rights of individuals and create more trustworthy A.I.¹²⁸ The current draft of the E.U. A.I. Act is still undergoing amendments as it passes through the European political channels, but the basic framework for A.I. classifications will be structured into a pyramid.¹²⁹ The classification takes an individual-centric approach, classifying A.I. according

¹²¹ *Id.* at 166–67 (“[Following WWII and] the establishment of the United Nations, many countries recognized that basic human rights needed to be protected to support democratic institutions . . . [T]he Council of Europe . . . [created] the European Convention on Human Rights.”). This piece of legislation emphasizes freedom of expression and privacy rights. *Id.*

¹²² W. Gregory Voss, *AI Act: The European Union’s Proposed Framework Regulation for Artificial Intelligence Governance*, 25 J. INTERNET L. 7, 7 (2021).

¹²³ *See id.* at 7–8.

¹²⁴ Kop, *supra* note 50, at 2.

¹²⁵ Voss, *supra* note 122, at 8.

¹²⁶ Kop, *supra* note 50, at 2.

¹²⁷ Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49.

¹²⁸ Voss, *supra* note 122, at 8 (discussing that the primary objectives of the E.U. A.I. Act are to ensure: (1) A.I. systems are safe and abide by pre-existing rights, values, and laws; (2) proper legal capacity to continue development of A.I.; (3) adequate enforcement of safety regulations and protection of fundamental rights; and (4) creation of a centralized, uniform market for safe and trustworthy A.I.).

¹²⁹ *See* Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49.

to the chance it has to affect the rights of individuals.¹³⁰ The bottom of the pyramid is “low-risk” A.I. and will encompass around “80 to 90% of all A.I.,” which will not be regulated.¹³¹ The following classification is “limited risk” A.I., which would face transparency requirements or no obligations, similar to low-risk.¹³² These A.I. fall into the non-high-risk category of the E.U. A.I. Act and, therefore, would only be subject to soft laws or none.¹³³ A.I. that qualifies as “high-risk” will require certain transparency, testing, and reporting requirements before being allowed onto the E.U. market.¹³⁴ High-risk A.I. has these requirements because of its likely potential impact on the rights of individuals, necessitating more stringent requirements.¹³⁵ At the top of the pyramid is “unacceptable risk” A.I. systems that the E.U. A.I. Act outright bans.¹³⁶ Examples of unacceptable risk applications include real-time facial recognition used in public spaces by governmental agencies and predictive policing.¹³⁷ The E.U. outright bans these because of the risk that they carry with their unpredictability and the risk of violating individuals’ fundamental rights.¹³⁸

Importantly, the E.U. A.I. Act also includes regulatory sandboxes: “controlled environment[s] to facilitate development, testing, and validation of innovative A.I. systems prior to placing them on the market or putting them into service.”¹³⁹ These sandboxes will

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² SABINE NESCHKE ET AL., ARTIFICIAL INTELLIGENCE POLICY AND THE EUROPEAN UNION 9 (2022), <https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2022/08/AI-Policy-and-EU-Final-Paper.pdf>.

¹³³ Voss, *supra* note 122, at 9 (“[High-risk] AI systems are subject to requirements set out in the proposed AI Act, while [non-high-risk AI systems] would not generally be regulated by the legislative proposal.”). Entities with non-high-risk A.I. systems are only encouraged to apply to the requirements for high-risk A.I. systems through soft laws and conduct codes. *Id.*

¹³⁴ Voss, *supra* note 122, at 11 (“Providers of high-risk AI systems are responsible for ensuring that the systems comply with requirements regarding a risk management system, data and data governance, technical documentation, record-keeping, transparency, and provision of information to users, human oversight, and accuracy, robustness, and cybersecurity.”).

¹³⁵ *Id.*

¹³⁶ NESCHKE ET AL., *supra* note 132, at 9.

¹³⁷ Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49.

¹³⁸ *Id.*

¹³⁹ Voss, *supra* note 122, at 14.

allow companies to test their products and scale them down or up before putting them onto the market to ensure they are in compliance. Co-rapporteur of the E.U. A.I. Act, Dragos Tudorache, noted that sandboxes allow for innovation and “encourage companies to come forward and actually test out their ideas in an environment that is free of risk of error.”¹⁴⁰ This sandbox structure also may encourage more effective legislation and compliance because the governments will be able to understand the reality companies face regarding compliance with the standards in place.¹⁴¹

While the Act is still in the early stages of European lobbying and policymaking, some version of the E.U. A.I. Act is likely to pass. The E.U.’s Executive Branch introduced the Act, indicating strong support for the Act’s passage into law.¹⁴² Once the Parliament and the Council reach a consensus on their views of the legislation, they will begin meeting in a “trialogue,” and the formal negotiations will begin for passing the E.U. A.I. Act into proper law.¹⁴³ Some version of the Act will likely pass within a few years.¹⁴⁴

The E.U. A.I. Act has some notable advantages over other proposed A.I. legislation. First, the E.U. A.I. Act requires specific A.I. systems, such as high-risk A.I., to submit to transparency requirements regarding the A.I.’s decisions.¹⁴⁵ These requirements remove the “black box” problem¹⁴⁶ that often accompanies A.I., leading to fairer outcomes for individuals and the protection of democratic due process concerns. Additionally, the E.U. A.I. Act would also create and maintain a publicly accessible database with information re-

¹⁴⁰ See Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49.

¹⁴¹ *Id.*

¹⁴² See Mökander et al., *supra* note 104, at 752–53.

¹⁴³ Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49. The European Council has reached a consensus on their view of the Act, which is now being proposed to the Parliament. See discussion *infra* Section III.B.

¹⁴⁴ Voss, *supra* note 122, at 14.

¹⁴⁵ *Id.* at 13 (explaining that high-risk A.I. systems like ones that interact with people must inform the people that they are A.I. and users of facial recognition software, and “deep fake” A.I. systems must inform the people they are targeting that they used facial recognition software).

¹⁴⁶ Manheim & Kaplan, *supra* note 1, at 155 (“Opaque AI outcomes are hidden by ‘black box’ algorithms. Since we often do not know how an AI machine reached a particular conclusion, we cannot test that conclusion for compliance with legal and social norms, whether the laws of war or constitutional rights.”).

garding these high-risk A.I. systems, allowing for more transparency.¹⁴⁷ The current draft of the proposed Act allows uniform application of its laws across the board, avoiding having member states interpret and apply the same rules differently.¹⁴⁸ Moreover, the Act's drafters have taken steps to protect individual fundamental rights and preserve democratic values, such as outright prohibiting certain uses of A.I.¹⁴⁹

Similar to the GDPR, the E.U. A.I. Act may also have a ripple or "Brussels Effect" that causes other countries to adopt similar A.I. legislation for "practical reasons."¹⁵⁰ The ripple effect would result in an extraterritorial effect on A.I. legislation in other countries like the U.S.¹⁵¹ This ripple effect has already begun in countries like Brazil with the passage of a legal framework for A.I. based on the proposed E.U. A.I. Act.¹⁵² Globalization's prevalence and the need for borderless legislation would allow companies to seamlessly comply with standards globally without the need to jump through different international legislative hoops.

However, the E.U. A.I. Act is facing some challenges and has areas that the Act's drafters need to fix. First, the initial draft of the Act defined A.I. very broadly as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs

¹⁴⁷ Voss, *supra* note 122, at 13.

¹⁴⁸ Kop, *supra* note 50, at 1–2.

¹⁴⁹ *Id.* at 2.

¹⁵⁰ Mökander et al., *supra* note 104, at 755–56. The "Brussels Effect" is a term attributable to the E.U.'s ability to influence other countries through shaping rules and technical standards. Peter L. Lindseth, *The Brussels Effect: How the European Union Rules the World*, 70 AM. J. COMPAR. L. 641, 641–45 (2023).

¹⁵¹ Manheim & Kaplan, *supra* note 1, at 178–79.

¹⁵² Eduardo Piovesan & Pierre Triboli, *Câmara Aprova Projeto que Regula o Uso da Inteligência Artificial [Chamber Approves Project that Regulates the Use of Artificial Intelligence]*, CÂMARA DOS DEPUTADOS (Sept. 29, 2021, 7:57 PM), <https://www.camara.leg.br/noticias/811702-camara-aprova-projeto-que-regulamenta-uso-da-inteligencia-artificial> ("According to the rapporteur [for Brazil's A.I. bill], the main inspiration for the changes comes from the proposal under discussion in the European Parliament and the Council for Europe for a new European legislation regarding artificial intelligence.").

such as content, predictions, recommendations, or decisions influencing the environments they interact with.”¹⁵³ This definition has led to strong debate among members of the E.U. that will be affected by the legislation because how it is tailored will allow for potential carveouts and result in either over-inclusivity or under-inclusivity.¹⁵⁴ Moreover, E.U. member states have proposed a “presidency compromise” draft, which offers a narrower definition of A.I. that allows for companies to easily argue that their software is not considered A.I.¹⁵⁵ While the definition is still in discussions within the E.U., one thing is clear: defining A.I. only leads to potential carveouts and hampering of the legislation.¹⁵⁶ Because the E.U. A.I. Act is attempting to define A.I. in a way that can meaningfully apply to all kinds of A.I. systems, this definitional issue is likely to be one of the downfalls of the Act when it is passed.

Another potential downfall of the Act is its proposed enforcement mechanisms. There are debates among legislators about whether national authorities or a centralized authority should enforce the regulations.¹⁵⁷ Currently, the proposal from the European Commission leaves the enforcement up to the respective national authorities, potentially resulting in states interpreting and enforcing the same law differently.¹⁵⁸ The proposal would be disastrous to companies’ compliance and result in the fragmented approach that the Act sought to avoid.¹⁵⁹ As supported by some parties, a central-

¹⁵³ *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*, at 39, COM (2021) 206 final (Apr. 21, 2021).

¹⁵⁴ Joanna J. Bryson, *Europe is in Danger of Using the Wrong Definition of AI*, WIRED (Mar. 2, 2022, 9:00 AM), <https://www.wired.com/story/artificial-intelligence-regulation-european-union> (“[A]bout half of the EU member states are pushing back against this broad definition.”).

¹⁵⁵ *Id.* (arguing that restricting the definition of A.I. to only sophisticated machine learning software would allow companies like Google to escape regulatory oversight and would undermine the purpose of the act).

¹⁵⁶ *See generally id.*

¹⁵⁷ Luca Bertuzzi, *Europe’s Artificial Intelligence Debate Heats Up*, CEPA (June 9, 2022), <https://cepa.org/article/europes-artificial-intelligence-debate-heats-up>.

¹⁵⁸ *See id.*

¹⁵⁹ Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49.

ized board would avoid this downfall and allow for uniform enforcement across the member states allowing for easier compliance and removing the legislative borders between the member states.¹⁶⁰

Lastly, debates over what practices are outright prohibited by and what carveouts are given to governmental agencies in the Act will likely slow down the legislative process for the Act. E.U. legislators have stated the most debated topics are what will qualify as prohibited practices¹⁶¹ and what carveouts are proscribed.¹⁶² This categorization issue could result in an ineffective Act if too many carveouts are given. The speed at which A.I. is growing requires such legislation to be versatile, and the passing of legislation without such a system in place would render it outdated and useless because of A.I.'s rapid growth.¹⁶³

III. CURRENT AND FUTURE IMPLICATIONS OF U.S. AND E.U. A.I. LEGISLATION

A. *What Is the Ideal Approach? Fragmentation or Centralization?*

Scholars and studies support the notion that centralized A.I. governance allows for more effective oversight, implementation, and adaptability, and encourages participation from members of society.¹⁶⁴ Fragmented approaches to regulation, such as multilateral international environmental agreements like the Kyoto Protocol, caused numerous problems with practical implementation, cost, participation, and “treaty congestion,” which could be the case for the U.S. and E.U. if the proper steps are not taken.¹⁶⁵

Centralized legislation, like the E.U. A.I. Act, has numerous benefits, such as encouraging political participation and efficiency,

¹⁶⁰ *Id.*

¹⁶¹ Bertuzzi, *supra* note 157. See Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49.

¹⁶² See Voss, *supra* note 122, at 10 (discussing that facial recognition systems are banned but are allowed by law enforcement when “‘strictly necessary’ for certain objectives”).

¹⁶³ See Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49.

¹⁶⁴ CIHON ET AL., *supra* note 47, at § 6.

¹⁶⁵ *Id.* at § 2.

reducing forum shopping, and encouraging policy coordination.¹⁶⁶ Centralized legislation would encourage political participation by allowing effective management, similar to the World Trade Organization's (WTO) agreements and regulations, which have influenced other countries' environmental legislation to conform to the WTO's agreements.¹⁶⁷ Secondly, centralization would likely encourage efficiency by reducing costs and avoiding having states allocate resources to different entities. Further, like the proposed E.U. A.I. Act, a centralized body of laws would remove conflicting and overlapping laws like international environmental agreements.¹⁶⁸ Additionally, centralization would remove forum shopping perpetuated by fragmented legislation, where actors and companies can selectively choose which states to participate in.¹⁶⁹ Lastly, it would likely facilitate policy coordination between member states in the E.U. with a centralized legislative body, allowing it to address policy issues arising from the constantly changing landscape of A.I.¹⁷⁰

However, at the same time, a centralized approach to regulation is not inherently better than a fragmented approach. A centralized approach has risks like creating a slow and rigid legislative body if the proper steps are not taken.¹⁷¹ Centralized legislation, such as the Paris Agreement of 2015, was diluted by numerous compromises when the Agreement attempted to "get all parties on board."¹⁷² The E.U. A.I. Act could face similar legislative weakening due to the challenge of getting agreement among all member states on specifics, such as the use of disputed facial recognition technology. Moreover, with a centralized approach, the risk of "slowness and brittleness" also means that the legislation may not adapt fast enough to the rapidly changing landscape of A.I.¹⁷³ For example, the General Agreement on Tariffs and Trade ("GATT") negotiations with the

¹⁶⁶ *Id.* at §§ 1–6.

¹⁶⁷ *Id.* at § 1.

¹⁶⁸ *Id.* at §§ 1–2.

¹⁶⁹ *Id.* at § 2.

¹⁷⁰ CIHON ET AL., *supra* note 47, at § 2.

¹⁷¹ *Id.* at § 3.

¹⁷² *Id.* at § 4 ("The 2015 Paris Agreement on Climate Change was significantly watered down to allow for the legal participation of the U.S. . . . [I]nclusion of the U.S. . . . came at the cost of significant cutbacks on the demands which the regime sought to make of all parties.").

¹⁷³ *See id.* at § 3.

Uruguay round “took 91 months to achieve a tariff reduction of 38% between 125 parties.”¹⁷⁴ However, amendments and proposals to the E.U. A.I. Act have recognized these risks.¹⁷⁵

On the other hand, fragmented legislation has some advantages, like the U.S.’s A.I. regulation approach. Firstly, the stakes are not as high, as failures—which will likely occur with A.I. legislation—are not as severe if they do occur.¹⁷⁶ For example, suppose one agency fails or missteps with regulating A.I. In that case, the impact will not be as severe as if the E.U. A.I. Act fails to identify a critical sector or defines A.I. incorrectly. Moreover, the fragmented approach allows for more specific definitions of A.I. instead of broad principles that can apply to every type of A.I., like the E.U. A.I. Act is attempting to do. Conversely, the U.S.’s sectoral approach allows agencies to tailor definitions to the application, as medical devices and mortgage approval A.I. will likely need different regulations or compliance requirements.¹⁷⁷ Additionally, the AAA and the A.I.BoR fail to empower agencies with the capacity or mandates they need—another shortcoming of fragmented approaches to regulation.¹⁷⁸

Overall, while a centralized approach to regulation presents high stakes and harsher outcomes if it fails, the benefits outweigh the risks. Although the E.U. A.I. Act is not an international agreement and only involves the member states in the E.U., it is the first step towards horizontal, centralized A.I. legislation.¹⁷⁹ As information about A.I. and the future of its development is scarce, a centralized piece of A.I. legislation encourages and ensures that information is readily available so the legislatures can amend or update the legislation as needed.¹⁸⁰ However, the E.U. A.I. Act is not without its downsides and areas of vulnerability. Indeed, the optimal approach

¹⁷⁴ *Id.*

¹⁷⁵ ACCESS NOW, JOINT CIVIL SOCIETY AMENDMENTS TO THE ARTIFICIAL INTELLIGENCE ACT: FUTURE PROOFING THE RISK-BASED APPROACH OF THE ARTIFICIAL INTELLIGENCE ACT 1–2, <https://www.accessnow.org/cms/assets/uploads/2022/05/Civil-Society-Amendments-on-Future-Proofing-the-Risk-based-Approach.pdf> (proposing amendments to numerous articles in the E.U. A.I. Act, ensuring it can be updated easily to future-proof it).

¹⁷⁶ CIHON ET AL., *supra* note 47, at § 3.

¹⁷⁷ *See* Engler, *supra* note 58.

¹⁷⁸ *See id.*

¹⁷⁹ *See generally* CIHON ET AL., *supra* note 47, at § 1.

¹⁸⁰ *See id.* at § 3.

to regulating A.I. is a combination of the U.S. and E.U.'s approaches.

B. *The Ideal Approach: A Combination of the U.S. and E.U.*

Although the U.S. and E.U. have started to recognize the need for adequate A.I. regulation going forward, there are a few areas where both entities can improve. In the past few years, over sixty countries have legislated some form of A.I. policy, which begs the question of uniformity and differing approaches.¹⁸¹ Moreover, the U.S. and E.U.'s approaches to regulation are also drastically different. As recognized by Tudorache and Research Fellow at the Brookings Institute, Alex Engler, the ideal approach is to ensure a similar global governance approach to A.I. policy.¹⁸² Ideally, the U.S., E.U., and other countries will adopt similar principles and norms that allow companies to develop without having different regulatory landscapes.¹⁸³ Collective approaches to A.I. are necessary to help fill the information deficit among legislators and guarantee effective A.I. legislation.¹⁸⁴ The information asymmetry between legislators and A.I. companies also calls for international collaboration and sharing of available information to ensure adequate regulatory oversight.¹⁸⁵

¹⁸¹ Alex Engler, *The EU and U.S. Are Starting to Align on AI Regulation*, BROOKINGS (Feb. 1, 2022), <https://www.brookings.edu/articles/the-eu-and-u-s-are-starting-to-align-on-ai-regulation>.

¹⁸² *Id.* (“[A] more unified . . . international approach to AI governance could strengthen common oversight, guide research to shared challenges, and promote the sharing of best practices, code, and data.”). See Interview by Gregory C. Allen with Dragos Tudorache, *supra* note 49 (discussing that the U.S., E.U., and other countries need to have a mutual understanding of A.I. policy with similar values such as the “rules, standards, and future work on AI.”).

¹⁸³ *Id.*

¹⁸⁴ CAMERON F. KERRY ET AL., STRENGTHENING INTERNATIONAL COOPERATION ON AI 3–4 (2021), https://www.brookings.edu/wp-content/uploads/2021/10/Strengthening-International-Cooperation-AI_Oct21.pdf (explaining how global cooperation is necessary to ensure “protection of democracy, freedom of expression, and other human rights,” as well as avoiding abusive uses of A.I. like China’s use that violates fundamental rights and stifles the research and development process of AI).

¹⁸⁵ Alex C. Engler, *A Bold Transatlantic Plan to Open Corporate Databases*, CEPA (July 8, 2021), <https://cepa.org/article/a-bold-transatlantic-plan-to-open-corporate-databases>.

The E.U.’s approach to regulating A.I. appears to be more effective. However, the ideal method for regulating A.I. would be a combination of the U.S.’s A.I.BoR, the AAA, and the E.U. A.I. Act. Firstly, the AAA and the A.I.BoR’s approach to defining A.I. is superior to the E.U. A.I. Act because both are “technology-agnostic,” ensuring they are future-proof.¹⁸⁶ Thus, future discussions concerning the E.U. A.I. Act should avoid focusing on the definition of A.I. and instead focus on the A.I. processes themselves.¹⁸⁷ Focusing on the processes themselves avoids one of the challenges of defining what A.I. is¹⁸⁸ and allows the regulatory authorities to focus on A.I. processes that threaten individual rights, like biometric scanning.¹⁸⁹

Moreover, the AAA’s focus on ADS instead of defining A.I. systems is more effective than the E.U.’s categorization approach. The AAA mandates transparency requirements to all ADS companies with a material impact on a user’s life.¹⁹⁰ In contrast, the E.U. A.I. Act only requires A.I. applications that qualify as high-risk to be subject to the transparency requirements and other regulations under the Act.¹⁹¹ These categorizations exclude around 90% of A.I. applications and overlook A.I.-supported “decision-making tasks” by only focusing on using A.I. alone.¹⁹² Thus, the E.U. A.I. Act should adopt the U.S.’s approach to ensure it does not overlook critical processes affecting users’ lives. While the E.U. A.I. Act’s risk-based approach ensures that regulations are aligned with the severity of the potential harm, it must be able to be adequately updated following developments in A.I.¹⁹³

However, the E.U. A.I. Act’s coverage model more adequately applies to all companies than the AAA or the A.I.BoR. The E.U. A.I.

¹⁸⁶ Mökander et al., *supra* note 104, at 752–53.

¹⁸⁷ *Id.* at 753 (“By focusing on regulating ‘critical decision processes’ rather than ‘high-risk AI systems,’ the U.S. AAA avoids the ontological question of what an AI system is . . .”).

¹⁸⁸ O’Shaughnessy, *supra* note 75 (noting that one of the most challenging topics around A.I. legislation is agreeing on a specific definition).

¹⁸⁹ *See id.*

¹⁹⁰ *Id.*

¹⁹¹ *Id.*

¹⁹² Mökander et al., *supra* note 104, at 753 (“[E]thical tensions do not emerge from using ADS alone but can also be related to the broader context of ADS-supported decision-making tasks.”).

¹⁹³ O’Shaughnessy, *supra* note 75.

Act applies to all companies, regardless of size, whereas the AAA only applies to certain companies¹⁹⁴ and the A.I.BoR only discusses existing agencies, leaving critical areas unaddressed.¹⁹⁵ Thus, the E.U. A.I. Act's model is ideal for ensuring that all companies using A.I. or ADS are subjected to the requirements of the legislation, regardless of size.

Further, A.I. legislation must be built to easily adapt to new and evolving A.I. technologies. The current proposals to the E.U. A.I. Act have recognized this with additions from the E.U. Council that include amendments to the definition of A.I. which specify the ability to update the definition for covered systems.¹⁹⁶ The ability to update ensures that the E.U. A.I. Act is "future-proof," which is necessary for A.I. in particular because of how fast it rapidly develops.¹⁹⁷ The current proposal submitted by the E.U. Council as of December 6, 2022, includes an amendment that explicitly allows for the addition and removal of high-risk A.I. cases.¹⁹⁸

Another lesson the U.S. can learn from the E.U. A.I. Act is the third-party conformity assessment requirements for high-risk A.I. systems.¹⁹⁹ Currently, the U.S.'s AAA only requires companies to

¹⁹⁴ Mökander et al., *supra* note 104, at 754 ("[The AAA] applies only to 'large companies' that either (a) have an annual turnover over \$50 million, (b) have over \$250 million in equity value, or (c) process the information of over 1 million users.").

¹⁹⁵ Engler, *supra* note 58 ("Important issues in educational access and worker surveillance, as well as most uses of AI in law enforcement, have received insufficient attention."); see GURSOY ET AL., *supra* note 97, at 4 (discussing that the AAA is limited to only entities within the FTC's jurisdiction and fails to cover "public agencies, banks, unions, air carriers, and common carriers" as well as credit agencies).

¹⁹⁶ *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, No. 14954/22, at 4 (Nov. 25, 2022) [hereinafter Proposed E.U. AI Act] ("To ensure that the AI Act remains flexible and future proof, a possibility to adopt implementing acts to further specify and update techniques under machine learning approaches and logic- and knowledge-based approaches has been added in Article 4.").

¹⁹⁷ See Finnbarr Toesland, *AI is Growing Fast - and Isn't Set to Slow Down*, TECHERATI (Dec. 10, 2021), <https://www.techerati.com/features-hub/opinions/ai-is-growing-fast-and-isnt-set-to-slow-down> (according to Stanford's 2019 A.I. index report, A.I. has been doubling every 3.4 months since 2012).

¹⁹⁸ Proposed E.U. AI Act, *supra* note 196, at 5.

¹⁹⁹ *Id.* at 34.

undergo self-assessments.²⁰⁰ These are inherently unreliable and give companies unlimited flexibility regarding the standards and reporting requirements they use to create their summary reports.²⁰¹ U.S. legislation such as the AAA should adopt principles similar to the E.U. A.I. Act and implement more funding and research to establish standards requiring independent third-party conformity assessments.²⁰² These principles would help prevent manipulative or biased reporting by A.I. companies.

Neither the AAA²⁰³ nor the A.I.BoR addresses the information deficit between the general public and companies that use A.I. The E.U. A.I. Act recognizes this information need by establishing a publicly accessible database for high-risk A.I. systems, providing relevant information about the high-risk systems in the market.²⁰⁴ As suggested by scholars, the AAA should adopt a proposed recommendation requiring the FTC to create an easy-to-read, publicly accessible database of summary reports for covered companies.²⁰⁵

A.I. legislation must have continuous monitoring and conformity assessments. The E.U. A.I. Act recognizes this as it requires detailed, continuous, conformity, and periodic assessments for the “entire lifecycle” of high-risk A.I. systems.²⁰⁶ While the AAA requires yearly summary reports to be submitted to the FTC,²⁰⁷ it does not require new reports for when A.I. systems change or deviate, leaving a lot of room for a potential negative impact on consumers.²⁰⁸ Thus, the AAA should adopt a similar approach to the E.U. A.I. Act by requiring companies to submit continuous summary reports and impact assessments to the FTC, especially when the approved behavior changes.²⁰⁹

²⁰⁰ Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 2–3 (2022).

²⁰¹ GURSOY ET AL., *supra* note 97, at 4.

²⁰² *Id.* at 5–6.

²⁰³ *Id.* at 6 (explaining that the AAA does not provide affected people with the necessary information about covered ADS systems except for the fact that it exists).

²⁰⁴ Proposed E.U. AI Act, *supra* note 196, at 157–58.

²⁰⁵ GURSOY ET AL., *supra* note 97, at 6.

²⁰⁶ Proposed E.U. AI Act, *supra* note 196, at 41.

²⁰⁷ Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 3 (2022).

²⁰⁸ GURSOY ET AL., *supra* note 97, at 6.

²⁰⁹ *Id.*

Lastly, the version of the E.U. A.I. Act proposed by the Council narrowed the definition of A.I.²¹⁰ Although the definition can be amended, this is a significant misstep for the Act, as limiting the definition allows companies to avoid regulation and was one of the greatest fears of the E.U. A.I. Act.²¹¹ This new proposed definition is already recognized as narrow, imprecise,²¹² and contrary to the legislation's goal.²¹³ As the Commission considers this newly proposed definition by the Council, they should consider the U.S.'s approach to defining A.I. However, the ideal approach would be to forego the definition of A.I. like the U.S.'s legislation²¹⁴ and UNESCO's legislation does,²¹⁵ and instead focus on the A.I. process itself to avoid overlooking violations of fundamental rights.²¹⁶ The best possible approach would be to combine the AAA's focus on the A.I. system's impact with the E.U.'s risk-based approach to regulating A.I.

Overall, the U.S. and E.U. both have favorable aspects of their approach to A.I. legislation thus far. The E.U.'s risk-based approach, centralized framework, publicly accessible database, and

²¹⁰ *Proposal for EU Artificial Intelligence Act Passes Next Level – Where Do We Stand and What's Next?*, SIDLEY AUSTIN LLP (Dec. 12, 2022), <https://www.sidley.com/en/insights/newsupdates/2022/12/proposal-for-eu-artificial-intelligence-act-passes-next-level> (summarizing the main elements of the compromise proposal as the compromise text narrows down the definition in Article 3(1) to developed through machine learning approaches and logic- and knowledge-based approaches).

²¹¹ *See id.* (“The council is in favor of a narrow definition, which may be further specified by the Commission so as not to capture all types of ‘traditional’ software.”); *see also* O’Shaughnessy, *supra* note 75.

²¹² *Proposal for EU Artificial Intelligence Act Passes Next Level – Where Do We Stand and What's Next?*, *supra* note 210.

²¹³ Bryson, *supra* note 154 (discussing that the narrow definition proposed by the compromise draft allows for “corruption and negligence,” as well as highly controversial practices “like social credit systems and generalized facial recognition in public spaces”).

²¹⁴ *See* discussion *supra* Section II.A.

²¹⁵ O’Shaughnessy, *supra* note 75 (“An influential UNESCO document forgoes a precise definition in favor of a focus on the impacts of AI systems, leading to a more future-proof instrument that is less likely to need to be updated as technology evolves.”).

²¹⁶ *Id.* (using definitions of A.I. that focus only on specific aspects ignore “real harms that result from the blind use of historical data in both complex and classical algorithms”).

ability to be continuously monitored are notable advantages that it has over the U.S.²¹⁷ U.S. legislation also has unique advantages by avoiding the definition of A.I. and its ability to closely regulate specific A.I. on an agency-by-agency basis.²¹⁸ However, the U.S.'s current A.I. legislation—the AAA, A.I.BoR—is not as comprehensive as the E.U. A.I. Act, leaving critical areas unaddressed, and is not thorough enough. The lack of comprehensiveness will allow dangerous A.I. to develop unregulated and corrode democratic values. Conversely, the E.U. A.I. Act is an extensive piece of A.I. legislation focused on protecting individuals' rights, hopefully influencing future U.S. legislation.

CONCLUSION

U.S. legislators should adopt the E.U.'s risk-based approach and emphasize comprehensive legislation, even if it makes compliance difficult.²¹⁹ However, while the AAA is not likely to pass,²²⁰ the A.I.BoR is seen as one step in the right direction toward the E.U.'s approach. While non-binding, the A.I.BoR is hopefully the Biden administration's first step towards the E.U.'s centralized approach to A.I. regulation. The first binding federal legislation we will likely see in the U.S. is federal data privacy legislation like the proposed American Data Privacy and Protection Act ("Data Protection Act").²²¹ Similar to how the GDPR was the precursor for the E.U. A.I. Act, the Data Privacy Act will likely be a precursor to additional federal A.I. legislation.

²¹⁷ See discussion *supra* Section II.B.

²¹⁸ See discussion *supra* Section II.A.

²¹⁹ See discussion *supra* Section II.B.

²²⁰ See Mökander et al., *supra* note 104, at 756 (finding that it is unlikely the AAA will pass because multiple versions of similar E.U. technology law failed in Congress with only "two pieces of federal technology legislation passing in the last 25 years").

²²¹ CONG. RSCH. SERV., OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 1 (2022), <https://crsreports.congress.gov/product/pdf/LSB/LSB10776>.

Conversely, some version of the E.U. A.I. Act will pass as it is in the final negotiations now and is predicted to become law sometime during the next year or two.²²² The E.U. Council has finalized its version of the E.U. A.I. Act with the abovementioned proposals as of December 6, 2022.²²³ Although the E.U. A.I. Act has certain flaws, it is the most comprehensive piece of A.I. legislation that is likely to become binding law in the near future. The Act would be even stronger if it adopted the proposed recommendations from U.S. legislation.²²⁴

A.I. legislation presents a formidable challenge for policymakers, as it is an ever-evolving and complex field with a significant information deficit. The rapid pace of technological advancements in A.I. requires legislators to stay abreast of the latest developments and the potential risks posed by the technology. Without proper regulation in place, A.I. has the potential to bring about either a technological revolution or a catastrophic downfall. The dangers of unregulated A.I. are far-reaching and have the potential to corrode democracy, society, and individual freedoms. It is imperative that legislators understand the unique nature of A.I. legislation and take a proactive approach to ensure effective regulation. Failure to do so could result in the loss of control over the technology, leading to negative consequences that may be irreparable. Above all, A.I. technology must be developed and deployed in a manner that benefits society and protects the rights of individuals.

Thus, policymakers in the U.S. and E.U. must develop A.I. legislation while taking into consideration the following: balancing innovation and protection, addressing ethical concerns, taking into account the pace of technological change, encouraging responsible development and deployment, ensuring accountability, promoting transparency, and aligning with international standards.²²⁵

²²² Laura De Boel et al., *Council of the EU Proposes Amendments to Draft AI Act*, WILSON SONSINI (Dec. 22, 2022), <https://www.wsgr.com/en/insights/council-of-the-eu-proposes-amendments-to-draft-ai-act.html>.

²²³ *Proposal for EU Artificial Intelligence Act Passes Next Level – Where Do We Stand and What’s Next?*, *supra* note 210.

²²⁴ See discussion *supra* Part III.

²²⁵ See discussions *supra* Sections II.A, II.B.