Missouri Law Review

Volume 89 | Issue 3 Article 6

Summer 2024

Bridging the Divide: Does the EU's AI Act Offer Code for Regulating Emergent Technologies in America?

Renee Henson

Bridging the Divide: Does the EU's AI Act Offer Code for Regulating Emergent Technologies in America?

Renee Henson[*]

ABSTRACT

The European Union ("EU") has taken the remarkable step of coming to agreement to implement the first-of-its-kind comprehensive legislation regarding artificial intelligence ("AI"), the AI Act. The AI Act adopts a risk-based approach to address diverse AI system applications and potential harms associated with AI technology. The AI Act categorizes AI systems based on risk levels, ranging from unacceptable to minimal, with corresponding regulatory requirements tailored to mitigate associated risks. Efforts are underway in the United States to establish AI regulatory frameworks, as demonstrated by the Bipartisan Framework for U.S. Act, proposed by Senators Josh Hawley (R-MO) and Richard Blumenthal (D-CT); the proposed No Section 230 Immunity for AI Act; and President Biden's Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, inter alia. This Article provides a synopsis of the final provisions adopted in the AI Act. The Article then explores United States policymakers' most recent efforts to establish a regulatory path that balances principles of innovation with risk mitigation.

*Visiting Assistant Professor of Law at the University of Missouri School of Law.

TABLE OF CONTENTS

I. INTRODUCTION

The European Union ("EU") has taken the remarkable step of coming to agreement by implementing the first-of-its-kind comprehensive legislation regarding artificial intelligence ("AI"), the AI Act.[1] The law has been years in the making and is a triumph of collaboration and ambition in light of the complexities, rapid evolution, and variable applications of AI technology. The AI Act has been adopted and will serve as a reference for other nations.[2]

The AI Act provides a commonsense risk-based tiered approach to addressing the harms associated with AI. AI systems with the greatest potential for harm are highly regulated—or banned in some cases—and AI tools with the lowest risk of harm are subject to less restrictive regulation.[3] The AI Act will restrict AI systems that present the highest risk of harm to society, contemplating a step-down approach involving fewer legal restrictions for less severe harms to society.[4]

Part II of this Article will describe the AI Act's structure and likely impact. Part II will also examine the widespread concern about the regulation's potential of stifling innovation through the lens of various stakeholders. Part III will then explore the United States' status toward developing a comprehensive legal structure to facilitate responsible AI systems use.

II. THE AI ACT – A SYNOPSIS

In late 2023, EU officials agreed on the draft language of the AI Act, which is the world's first comprehensive regulation concerning applied AI technology.[5] The European Parliament approved the legislation on March 13, 2024.[6] Five-hundred and twenty-three Members of Parliament endorsed a

---

[1] *The AI Act Enters Info Force*, EUR. COMM'N (Aug. 5, 2024), https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en?utm_source=substack&utm_medium=email [https://perma.cc/TW9S-KQN7]; *see Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI*, EUR. PARL. (Dec. 9, 2023, 12:04 AM), https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai [https://perma.cc/RG4F-TYSZ].

[2] *See generally* Martin Coulter, *What is the EU Act and When Will Regulation Come into Effect?*, REUTERS (Dec. 7, 2023, 8:01 AM), https://www.reuters.com/technology/what-are-eus-landmark-ai-rules-2023-12-06/ [https://perma.cc/6KQC-HV4U].

[3] *Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI*, *supra* note 1.

[4] *Id.*

[5] *Id*.

[6] *Artificial Intelligence Act: MEPs Adopt Landmark Law*, EUR. PARL. (Mar. 13, 2024, 12:25 PM), https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law [https://perma.cc/9Y3X-

provisional agreement in favor of the AI Act; with only forty-six votes against it and forty-nine abstentions.[7] The AI Act went into effect on August 1, 2024.[8]

Much of the AI Act will take full effect within the next 24 months; however, some provisions will be in effect sooner and others later.[9] For example, regulation regarding AI systems that present unacceptable risks will take effect within six months, while provisions applicable to general-purpose AI will take effect within 12 months.[10] Studies, white papers, public consultation, draft proposals, impact assessments, and input from various stakeholders preceded the AI Act's adoption.[11] The AI Act's purpose may be summarized as ensuring compliance with existing laws, encouraging innovation by securing predictability in the law, guaranteeing that fundamental rights are respected, and supporting a legal and responsible market for the proliferation of safe AI application use.[12]

A. The Risk Categories Adopted

The AI Act sets forth a risk-based tiered regulatory approach.[13] This approach establishes legal requirements in proportion to an AI-system's level of risk to the public.[14] The term "artificial intelligence system" is difficult to

AE2G]; Isabel Gottlieb, *EU Poised to Enact Sweeping AI Rules With US, Global Impact*, BLOOMBERG LAW (Mar. 6, 2024, 11:24 AM), https://news.bloomberglaw.com/product/blaw/bloomberglawnews/exp/eyJpZCI6IjAwMDAwMThkLWFmZDAtZDU0OS1hZGJmLWFmZGNmMWRkMDAwMCIsImN0eHQiOiJCVU5XIiwidXVpZCI6IjdtSmZDNUV1MXFuRk9McHlKaTdkMkE9PUNVMHlTL3R1VngxQU5KeGx5TjFTVHc9PSIsInRpbWUiOiIxNzA5NzMwOTE4ODY2Iiwic2lnIjoiakZhOWFFQ0pRVlNVSWI1OER5TVZEL2dUUVdjPSIsInYiOiIxIn0=?source=newsletter&item=body-link&region=text-section [https://perma.cc/7FDZ-9B3Z].

[7] *Artificial Intelligence Act: MEPs Adopt Landmark Law, supra* note 6.

[8] *The AI Act Enters Info Force*, *supra* note 1.

[9] *Id.;* Regulation (EU) 2023/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, art. 113 [hereinafter AI Act] ("This Regulation shall . . . apply from 2 August 2026. However: (a) Chapters I and II shall apply from 2 February 2025; (b) Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101; (c) Article 6(1) and the corresponding obligations in this Regulation shall apply from 2 August 2027.").

[10] *The AI Act Enters Info Force*, *supra* note 1.

[11] Tambiama Madiega, *Briefing EU Legislation in Progress on Artificial Intelligence Act*, EUR. PARL. 2 (Mar. 2024), https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf [https://perma.cc/Q9DP-UEWS].

[12] *See generally id.* at 3–4.

[13] *Id.* at 1; *see* AI Act, *supra* note 9.

[14] Madiega, *supra* note 11, at 1.

define due to its amorphous qualities and myriad applications.[15] Under the AI Act, the term is defined as:

> [A] machine-based system . . . designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[16]

This definition ostensibly includes both narrow AI (single-tasked based) and machine-based learning AI (complex with capabilities to learn how to complete assigned tasks).[17]

The AI Act is broad in scope; it applies to AI systems ex-ante and ex-post.[18] It also applies to providers that operate their AI systems within EU's stream of commerce, regardless of the provider's physical base of operation.[19] Thus, the extraterritorial implications of the AI Act's broad scope will reverberate throughout other countries.[20] The tiered risk levels that this Article addresses are: unacceptable risk; high risk; general-purpose and generative AI; transparency obligations and minimal risk systems.[21]

---

[15] *See* STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 1–4 (4th ed. 2022); RAYMOND KURZWEIL, THE AGE OF INTELLIGENT MACHINES (MIT Press, 1990); Pei Wang, *On Defining Artificial Intelligence*, 10 J. ARTIFICIAL GEN. INTEL. 1, 1–37 (2019); David T. Laton, *Manhattan_Project.exe: A Nuclear Option for the Digital Age*, 25 CATH. U. J.L. & TECH. 94 (2016) (several definitions include "programs designed to think like humans, programs designed to think rationally, programs designed to act like humans, and programs designed to act rationally.").

[16] AI Act, *supra* note 9, at art. 3(1).

[17] WOODROW BARFIELD & UGO PAGALLO, ADVANCED INTRODUCTION TO LAW AND ARTIFICIAL INTELLIGENCE 5 (Stephen Harris ed., 2020); Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J. L. & TECH. 889, 898 (2018).

[18] Madiega, *supra* note 11, at 8–9 (stating providers must adhere to the AI Act both before their products are introduced into the stream of commerce and ensure continued compliance once introduced). For example, a provider of a high-risk AI-enabled system "shall document its assessment before that system is placed on the market or put into service." AI Act, *supra* note 9, at ch. III, § 1, art. 6(4).

[19] A provider is defined as "a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system . . . developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge[.]" AI Act, *supra* note 9, at ch. I, art. 3(3).

[20] *See* Madiega, *supra* note 11, at 7.

[21] *Id.* at 1; AI Act, *supra* note 9, at ch. II, ch. III, ch. IV, ch. V; *High-Level Summary of the AI Act*, EU ARTIFICIAL INTELLIGENCE ACT (Feb. 27, 2024),

1. Unacceptable Risk

An unacceptable risk is completely prohibited pursuant to the AI Act.[22] Several categories of AI systems are banned due to this risk level designation.[23] The AI Act prohibits the service or distribution of AI systems that deploy the following subliminal techniques:

> [B]eyond a person's consciousness or [are] purposefully manipulative or [use] deceptive techniques, with the objective to or the effect of materially distorting a person's . . . behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that [the] person would not have otherwise taken . . . in a manner that causes or is likely to cause . . . significant harm.[24]

Although AI "subliminal techniques" may appear as an unrealized dystopian concern, there are several ways that AI systems can covertly manipulate consumer behavior.[25]

For example, one study showed that subliminal stimuli using low-frequency seat vibrations improved drivers' behaviors.[26] The European Commission has proposed a hypothetical illustration "where an inaudible sound is played in a truck driver's cabin, which pushes the driver to continue longer than is healthy or safe."[27] Similar non-subliminal—but nonetheless covert—techniques are being used.[28] Uber "nudges" drivers to continue driving by notifying them that they are close to reaching monetary goals.[29] This technique encourages drivers to continue working by "framing the

---

https://artificialintelligenceact.eu/high-level-summary/ [https://perma.cc/YLZ5-FNFH]; 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, 2021/0106 (COD), at 3–10, 164–66.

[22] Madiega, *supra* note 11, at 3.

[23] AI Act, *supra* note 9, at ch. II.

[24] *Id*. at ch. II, art. 5(1)(a).

[25] *See* Matija Franklin et al., *Vague Concepts in The EU AI Act Will Not Protect Citizens From AI Manipulation*, OECD.AI POL'Y OBSERVATORY (Sept. 7, 2023), https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions [https://perma.cc/NGW2-2XHU].

[26] Juan Pablo Bermúdez et al., *What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence*, 2023 IEEE INTERNATIONAL SYMPOSIUM ON ETHICS IN ENGINEERING, SCIENCE, AND TECHNOLOGY (ETHICS) (forthcoming 2024) at 2, accessible at https://www.researchgate.net/publication/371906314_What_Is_a_Subliminal_Technique_An_Ethical_Perspective_on_AI-Driven_Influence [https://perma.cc/FV9R-LCVV].

[27] *Id.*

[28] *Id.* at 4.

[29] *Id.* at 3.

decision to log off as a loss," a persuasive psychological technique shown to influence individuals' behaviors.[30] Thus, AI systems using subliminal techniques and subliminal-adjacent techniques present a current issue.

The AI Act also prohibits the service or distribution of AI systems that can take advantage of vulnerable populations, including:

> [E]xploit[ing] any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is reasonably likely to cause . . . significant harm.[31]

Another class of banned AI includes systems that classify individuals based on biometric data through biological categorization systems with the intent to determine "race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation."[32]

There are many AI-enabled technologies that currently use biometric data in unexpected ways.[33] For example, some biometric technologies can detect "heart beats and brain waves via EEG or ECG, [leading to] the development of brain-computing interfaces . . . [, which] measure neuro activity and translate brain activity into machine-readable input."[34] This type of biometric data may permit one to infer a person's thoughts, intentions, emotions, or stress levels.[35] AI-enabled technologies generally raise fundamental rights issues, such as data privacy and protection, non-discrimination, equal access to justice, and consumer protection, *inter alia*.[36]

---

[30] *Id.*

[31] AI Act, *supra* note 9, at ch. II, art. 5(1)(b).

[32] *Id.*; *id.* at ch. II, art. 5(1)(g).

[33] Christiane Wendehorst & Yannic Duller, *Briefing Requested by the JURI and PETI Committees: Biometric Recognition and Behavioural Detection, Assessing the Ethical Aspects of Biometric Recognition and Behavioral Detection Techniques with a Focus on Their Current and Future Use in Public Spaces*, EUR. PARL. 1, 2 (Sept. 2021), https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI(2021)697131_EN.pdf [https://perma.cc/Z2AU-92UB].

[34] *Id*. at 2. Electroencephalograms ("EEG") and Echocardiograms ("ECG") measure electrical activity in the brain and cardiovascular system, respectively. *Id.*; *see* ERIC K. ST. LOUIS ET AL., ELECTROENCEPHALOGRAPHY (EEG): AN INTRODUCTORY TEXT AND ATLAS OF NORMAL AND ABNORMAL FINDINGS IN ADULTS, CHILDREN, AND INFANTS (Erik K. & Lauren C. Frey eds., 2016). Recent advances in the sensor technology have permitted EEG and ECG signals to be highly detectable. *See* Wendehorst & Duller, *supra* note 33; ST. LOUIS ET AL., *supra* note 34.

[35] Wendehorst & Duller, *supra* note 33, at 3.

[36] *Id*. at 3–4; *see Getting the Future Right: Artificial Intelligence and Fundamental Rights*, EUR. UNION AGENCY FOR FUNDAMENTAL RTS. 5 (2021), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_en.pdf [https://perma.cc/3HVF-Q4D2].

Nonetheless these capabilities derived from biometric data have generated interest in establishing new fundamental individual "neuro-rights."[37] Fundamental neuro-rights are beyond the scope of this Article, but the concept is likely to have increased significance as AI systems continue to become more sophisticated.

The AI Act also prohibits the servicing or distribution of AI systems that categorize individuals based on social classification, behavior, or personal characteristics for the purposes of creating a "social score."[38] A publicly recognized social score could result in disparate treatment "in social contexts that are unrelated to the contexts in which the data was originally generated . . . [or] that is unjustified or disproportionate to their social behaviour or its gravity."[39] This prohibition calls to mind China's mysterious social credit system, which incentivizes and punishes individuals based on their "state-sanctioned moral values" as a part of China's social scoring milieu.[40]

Notably, although the Chinese *central* government is developing draft regulation to establish a social credit system that rewards positive action and punishes undesirable action, it does not have a "central social credit score for individuals."[41] That said, *local* Chinese governments have done exactly that, issuing social scores, or "grades," to individuals that fluctuate based on their desirable and undesirable social actions.[42] For example, an individual may raise their social score by winning a sports competition, and lower it by communicating about a commercial dispute.[43] And although the Chinese social scoring system is said to be presently rudimentary in its technical capabilities, the concept of social scoring using AI systems has led to widespread concern.[44] This concern is reflected in the AI Act's complete social scoring ban.[45]

The AI Act creates an outright ban on "real-time" biometric tracking in public spaces for law enforcement's use, although policymakers created carve-outs for the following purposes:

---

[37] Wendehorst & Duller, *supra* note 33, at 4. Neuro-rights may be defined as "a category of rights aimed at the protection of the minds of citizens" including "[t]he right to mental privacy," "[t]he right to mental identity," "[t]he right to agency or free will," and the "general right to equality and justice in a context in which mental augmentation is part of our lives." Rafael Yuste, *Neuro-Rights and New Charts of Digital Rights: A Dialogue Beyond the Limits of the Law*, 30 IND. J. GLOBAL LEGAL STUDS. 15, 23–24 (2023).

[38] AI Act, *supra* note 9, at ch. II, art. 5(1)(c).

[39] *Id.*

[40] Zeyi Yang, *China Just Announced a New Social Credit Law, Here's What it Means*, MIT TECH. REV. (Nov. 22, 2022), https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/ [https://perma.cc/QVS7-S4QK].

[41] *Id*.

[42] *Id*.

[43] *Id*.

[44] *Id*.

[45] *See id*.; Wendehorst & Duller, *supra* note 33, at 3.

> [U]nless and in so far as such use is strictly necessary for . . . the targeted search for victims of abduction, trafficking in human beings or sexual exploitation [and in the] search for missing persons . . . the prevention of a specific substantial, and imminent threat to life or physical safety [or there is a] genuine and present or genuine and foreseeable threat of a terrorist attack . . . or identification of a person suspected of having committed a criminal offence, for the purposes of conducting a criminal investigation or prosecution or executing criminal penalty for offences . . . .[46]

This ban generated controversy, stalling implementation of the AI Act due to some lawmakers' concerns for protecting citizens' rights to privacy, at odds with other member states' concerns for protecting national security interests.[47] Because real-time biometric identification tools create a potential risk for problematic and discriminatory uses, this ban created a roadblock that stalled the AI Act's adoption in late 2023.[48] Real-time biometric identification systems arose as a point of contention among lawmakers regarding law enforcements' desired use of biometric AI applications, particularly for use in limited contexts like matters of national security and border security.[49] These points of contention were resolved by incorporating several carve-outs—as stated, in part, above—to an outright ban on real-time biometric system use.[50]

Included in this prohibition is a ban on AI systems that make risk assessments to predict the chances of a person committing a future crime—also known as "predictive policing."[51] The government can, however, use these real-time biometric systems when *humans* are involved in assessing the risk of potential likelihood of committing a future offense.[52] Additionally, providers are prohibited from using AI systems that expand on facial recognition databases that source "facial images from the internet or CCTV footage" as well as systems that can "infer [individuals'] emotions" when used in work or educational environments, except where those systems are used "for medical or safety reasons."[53]

---

[46] AI Act, *supra* note 9, at ch. II, art. 5(1)(h).

[47] *See* Coulter, *supra* note 2.

[48] *See id*.

[49] *Id.*

[50] AI Act, *supra* note 9, at ch. II, art. 5(1)(h). "'[R]eal-time' remote biometric identification system' means a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, compromising not only instant identification, but also limited short delays in order to avoid circumvention[.]" *Id.* at ch. I, art. 3(42).

[51] *Id.* at ch. II, art. 5(1)(d).

[52] *Id.*

[53] *Id.* at ch II, art. 5(1)(e)–(f).

2. High Risk

Article 6 of the AI Act provides that high-risk AI systems are those explicitly listed in the Union Harmonisation Legislation and those that are "required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union Harmonisation legislation."[54] The AI systems referenced in this legislation include, but are not limited to, the following:

- Aviation products using AI systems;
- Medical devices using AI systems;
- Motor vehicles using AI systems;
- Biometric identification AI systems;
- AI systems used "in the management of critical digital infrastructure . . . road traffic and the supply of water, gas, heating and electricity";
- AI systems used in education, whether in admissions or in determining students' learning outcomes "at all levels," or in overseeing students' behavior;
- AI systems used to identify and hire putative employees, including AI systems used to post job information and to make any decision impacting workers' promotion, hiring, firing, work allocation tasks, or performance evaluations;
- AI systems that impact individuals' access to "public assistance benefits and services," or AI systems that impact individuals' credit scores;
- AI systems that identify and dispatch emergency services to those in need of emergent care or police or firefighters' services;
- AI systems used by law enforcement in the form of lie detectors, evidence investigation, risk profiling, migration and border control management; and
- AI systems that impact the judicial system and democracy, including those that assist the judiciary in legal research, and those that may be used to influence elections.[55]

AI systems subject to high risk classification must engage in a "continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system" that entails identification of "known and . . . foreseeabl[e] risks"; a determination of risks that may arise from foreseeable use and misuse; and continuous risk management designed to "address the risks identified . . . ."[56] The AI Act specifies the risk management measures that affected providers should adhere to, including AI system testing.[57]

---

[54] *Id.* at ch. III, § 1, art. 6(1).

[55] *Id.* at ch. III, § 1, art. 6(1), Annex I, III.

[56] *Id.* at ch. III, § 1, art. 9(2).

[57] *Id.* at ch. III, § 2, art. 9.

High-risk products are also subject to data governance measures that require compliance with data collection processes and an "examination . . . of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination . . . ."[58] Data governance includes providers ensuring implementation of bias detection and prevention measures.[59] These bias requirements are important because of AI's widely studied and replicated proclivity to generate biased results.[60]

Importantly, the AI Act requires that before a high-risk product is placed into the stream of commerce, its creators provide "technical documentation" of the product and demonstrate that the AI system meets the AI Act's standards.[61] This technical documentation must provide the specific information requested in a "clear and comprehensive form."[62] AI system providers are further required to keep specific log records of the AI system's function for the "duration of the lifetime of the system."[63]

Moreover, AI systems must be transparently designed to allow for output interpretation.[64] Transparency includes: providing detailed information regarding the AI system's capabilities, "accuracy," "robustness," "cybersecurity" metrics, and many other factors.[65] The AI Act's transparency provisions are rigorous, likely requiring experts (including lawyers) and individuals with technical expertise in the development phase to ensure compliance. One AI compliance specialist stated, "I probably can't stress this enough: Organizations need to get started as soon as they possibly can . . . . It's not going to be very pretty if they wait until right before enforcement to start trying to implement all of the requirements."[66] Obtaining transparency, however, may be impossible for some AI systems with incomprehensible processes due to the ubiquitous "black box" problem.[67] In addition to transparency requirements, AI systems that fall into this category must have human oversight, meaning that they are designed in a way that can "be

---

[58] *Id.* at ch. III, § 2, art. 10(f).

[59] *Id.* at ch. III, § 2, art. 10(g).

[60] *See generally* Nicole K. McConlogue, *Discrimination on Wheels: How Big Data Uses License Plate Surveillance to Put the Brakes on Disadvantaged Drivers,* 18 STAN. J. C.R. & C.L. 279 (2022); Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCIENCE 447 (2019).

[61] AI Act, *supra* note 9, at ch. III, § 2, art. 11.

[62] *Id.* Of practical import, small businesses and start-ups may provide the required information in simplified form. *Id.*

[63] *Id.* at ch. I(71).

[64] *Id*. at ch. I(72).

[65] *Id*. at ch. III, § 2, art. 13(3)(b).

[66] Gottlieb, *supra* note 6 (quoting Ryan Donnelly, co-founder of Enzai, a Belfast-based AI compliance company).

[67] Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J. L. & TECH. 106, 153–58 (2019).

effectively overseen by natural persons . . . ."[68] Another potential impossibility due to the black box problem.[69]

Finally, high-risk systems are required to be "developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and . . . perform consistently in those respects throughout their lifecycle."[70] Notably, there are many other requirements imposed on high-risk AI systems' providers and deployers.[71] Additionally, and as mentioned above, foreign importers and distributors are required to conform to the AI Act.[72] Providers that meet all of these requirements will receive an "EU declaration of conformity . . . ."[73] The AI Act's provisions regarding high-risk AI systems propose a pragmatic, if not demanding, schedule of laws that providers and all entities along the AI value chain must adhere to. In applying these widespread provisions to high-risk AI systems, the AI Act takes a comprehensive approach, addressing many risks associated with AI.

Article 6 of the AI Act also creates necessary oversight in the form of local government bodies established to administer and assist providers to ensure compliance.[74] Although it is likely that the AI Act's implementation will generate extensive litigation relating to the vagueness of the regulatory structure as applied, policymakers have done a remarkable job in drafting initial legislation that addresses a broad array of factors—a feat that is particularly challenging given AI systems' varied uses across many different sectors of society.

3. General-Purpose and Generative AI

Although the EU ultimately adopted the AI Act, the pace of enactment slowed in December of 2023 because of policymakers' inability to agree on issues regarding general-purpose and generative AI uses, *inter alia*.[75] EU

---

[68] AI Act, *supra* note 9, at ch. III, § 2, art. 14.

[69] Manheim & Kaplan, *supra* note 67, at 153–58. The black box problem describes the unknowable quality of certain AI systems. *Id*. Some AI systems' processes, conclusions, and decisions are not known, testable, or verifiable. *Id*.

[70] AI Act, *supra* note 9, at ch. III, § 2, art. 15.

[71] *Id.* at ch. III (The "other requirements" are plentiful and beyond the scope of this Article). The term, "Deployer" is defined as "a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity[.]" *Id.* at ch. I, art. 3(4).

[72] *Id.* at ch. I, art. 3. The term, "Importer" is defined as "a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country." *Id.* at ch. I, art. 3(6). "Distributor" is defined as "a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market." *Id.* at ch. I, art. 3(7).

[73] *Id.* at ch. III, § 3, art. 22(3)(b).

[74] *Id.* at ch. III, § 4, art. 28.

[75] Coulter, *supra* note 2.

policymakers could not agree on generative AI proposals because, with the introduction of ChatGPT-3 in 2022, generative AI swiftly presented significant problems that had not yet arisen before large language models emerged in the public domain.[76]

The EU's AI Act structure for regulating generative AI models would require companies to make records of training processes to show company efforts made to limit the risks of generative AI.[77] This structure would also require companies to submit to third-party audits.[78] Several powerful countries disagreed with this approach on the basis that companies should have the ability to regulate themselves, arguing that any additional regulation would restrict competition with non-regulated countries, like the United States.[79] The European Parliament has maintained that the proposed rules for generative AI systems are necessary and that any industry exception would create inconsistencies with other regulations that significantly restrict smaller businesses.[80] This disagreement was ultimately resolved with a compromise between lawmakers: providers producing general-purpose AI systems with systemic risks, such as the ability to interfere with government elections, impact economic security, and affect public health and safety, will be subject to additional regulations.[81]

Providers of general-purpose AI that do not pose systemic risks must maintain "technical documentation of the model, including its training and

---

[76] *Id.* Chat GPT-3 was created by Open AI and was preceded by Chat GPT-1 and Chat GPT-2. Amy B. Cyphert, *A Human Being Wrote This Law Review Article: GPT-3 and the Practice of Law*, 55 U.C. DAVIS L. REV. 401, 409–10 (2021). Chat GPT-3 is a large language model AI system that uses predictive text to complete impressive commands. *Id.*

[77] Coulter, *supra* note 2.

[78] *Id.*

[79] *Id.*

[80] Luca Bertuzzi, *EU Countries Give Crucial Nod to First-of-a-Kind Artificial Intelligence La*w, EURACTIVE (Feb. 15, 2024), https://www.euractiv.com/section/artificial-intelligence/news/eu-countries-give-crucial-nod-to-first-of-a-kind-artificial-intelligence-law/https://www.euractiv.com/section/artificial-intelligence/news/eu-countries-give-crucial-nod-to-first-of-a-kind-artificial-intelligence-law/ [https://perma.cc/4JGA-2ZZP]. These restrictions are outlined in the above-referenced regulations in this Section.

[81] AI Act, *supra* note 9, at ch. 1(110), ch. V. A general-purpose AI system that presents systemic risks is defined in the AI Act. *See id.* at ch. 1(110), ch. V. One factor considered in the definition is computing power as measured by floating point operations per second ("FLOPS"). *Id*. at ch. 1(110), ch. V. FLOPS are "[t]he performance capabilities of supercomputers . . . expressed using a standard rate for indicating the number of floating-point arithmetic calculations systems can perform on a per-second basis." James T. Gray*, Brain Chips and Whole Brain Emulation Could Ensure Football's Survival: Is It Worthwhile?*, 32 MARQ. SPORTS L. REV. 49, 77 n.29 (2021). The AI Act instructs that a FLOPS metric should be set, and if this metric is met by the computing power, it will be presumed that the system is a general-purpose AI with systemic risk and deserving of additional oversight. AI Act, *supra* note 9, at ch. V, § 1.

testing process and the results of its evaluation . . . ."[82] Moreover, these providers are required to produce this information to third-party providers that integrate the AI system into their own system "[w]ithout prejudice to the need to observe and protect intellectual property rights and confidential business information or trade secrets" so that these third-party providers may understand the capabilities of the generative AI system they themselves rely on.[83]

Providers of general-purpose AI that pose systemic risks, however, must adhere to stricter requirements. These providers must meet the general-purpose AI systems' requirements stated above as well as conduct a "model evaluation in accordance with standardised protocols and tools . . . including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks . . . . "[84] These providers must also report to the AI Office and/or national authorities regarding "serious incidents and possible corrective measures to address [any potential incidents] . . . ."[85] Other provider requirements include maintaining adequate cyber security protection and assessing possible risks along with their source information.[86]

These requirements—and others within the AI Act—raise questions regarding how providers will balance the competing demands to comply with the regulation when successful implementation seems dubious. It is well known that current general-purpose AI systems have *already* been trained on copyright protected material. The legality of generative AI systems using copyrighted material to train their systems is pending across jurisdictions within the United States.[87] EU lawmakers have acknowledged the challenges that lay ahead with respect to the AI Act's successful implementation:

> The EU has delivered. We have linked the concept of artificial intelligence to the fundamental values that form the basis of our societies. However, much work lies ahead that goes beyond the AI Act itself. AI will push us to rethink the social contract at the heart of our democracies, our education models, labour markets, and the way we conduct warfare. The AI Act is a starting point for a new model of governance built around technology. We must now focus on putting this law into practice.[88]

---

[82] AI Act, *supra* note 9, at ch. V, § 2, art. 53(1).

[83] *Id.*

[84] *Id.* at ch. V, § 3, art. 55(1).

[85] *Id.*

[86] *Id.*

[87] *See* Complaint for Petitioner, New York Times Co. v. Microsoft Corp., Case 1:23-cv-11195, 2023 WL 9750489 (S.D.N.Y. Dec. 27, 2023); Andersen v. Stability AI Ltd., Case 3:23-cv-00201, 2023 WL 7132064 (N.D. Cal. Oct. 30, 2023), *inter alia*.

[88] *Artificial Intelligence Act: MEPs Adopt Landmark Law*, *supra* note 6 (quoting Civil Liberties Committee Co-Rapporteur Dragos Tudorache of Renew, Romania).

Indeed, the true efficacy of the AI Act will be borne out in its implementation. The AI Act's goals for high-risk AI systems are lofty in what they hope to accomplish, and the challenges to its successful application are tremendous.

4. Transparency Obligations and Minimal Risk AI Systems

Other classifications under the EU's AI Act include transparency obligations and minimal risk AI systems.[89] Other "certain AI systems" are subject to few regulations and include media content like chatbots and deepfake technology.[90] For example, providers of AI systems that create or manipulate video images must inform users only that they are using an AI system or disclose that the media content is a manipulated "deep fake."[91] The AI Act permits almost unrestricted use of AI that poses minimal risk, such as AI systems incorporated into videogames or spam filters.[92]

Aside from the risk-based regulatory scheme, the AI Act encourages providers to experiment with new technology. Acknowledging the potential that these comprehensive regulations may stifle innovation, the AI Act establishes regulatory sandboxes whereby providers may test and develop AI systems before they are placed into the stream of commerce.[93] The stated purposes of the AI sandboxes are to "foster[] innovation and competitiveness and facilitate[e] the development of an AI ecosystem . . . ," *inter alia*.[94]

The AI Act's tiered approach to regulating AI systems is comprehensive, with the bulk of the restrictions placed on AI systems that pose unacceptable and high risks to society. Notably, critics have pointed to the estimated

---

[89] AI Act, *supra* note 9, at ch. IV; *High-Level Summary of the AI Act*, *supra* note 21; *EU AI Act: First Regulation on Artificial Intelligence*, EUR. PARL. (June 18, 2023, 4:29 PM), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence [https://perma.cc/5BNJ-5GEB].

[90] AI Act, *supra* note 9, at ch. IV, art. 50; *High-Level Summary of the AI Act*, *supra* note 21.

[91] AI Act, *supra* note 9, at ch. IV, art. 50(4) ("Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work."). A "deep fake image" is defined as an "AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful."). *Id.* at ch. I, art. 3(60).

[92] *High-Level Summary of the AI Act*, *supra* note 21.

[93] AI Act, *supra* note 9, at ch. VI, art. 57.

[94] *Id.* at ch. VI, art. 57(9)(c).

compliance and maintenance costs as a significant problem with the AI Act.[95] These concerns are likely the largest barrier to other countries seeking to adopt similar comprehensive measures.

B. Stakeholders' Objections to the AI Act

The AI Act has been described as "a regulation with teeth."[96] A violation of the AI Act is met with steep financial penalties.[97] For example, non-compliance with the unacceptable risk provisions may subject providers to fines up to thirty-five million EUR or a maximum of 7% their "total worldwide annual turnover for the preceding financial year, whichever is higher."[98] The penalties are meant to be proportionate, accounting for the providers' "economic viability"; however, they reflect lawmakers' intention to penalize violating providers of all sizes and relative wealth.[99] For many companies, these steep financial sanctions pose an existential risk and, at the bare minimum, may dampen AI research and development capabilities.

The European Commission drafted an impact study to assess the AI Act's effect on stakeholders.[100] The impact assessment found that to develop one "AI product," compliance costs are estimated at 29,277 EUR.[101] The aggregate compliance costs across all markets are estimated to be from 1.6 to 3.3 billion EUR.[102] The costs to certify a regulated "AI product through conformity assessment" is estimated to cost from 16,800 to 23,000 EUR, and developing a quality management system is estimated to cost anywhere from 193,000 to 330,000 EUR upfront and 71,400 EUR in annual maintenance costs.[103]

Unsurprisingly, some interested stakeholders have criticized the AI Act as being "likely to stifle investment and innovation [and argue] that soft measures like codes of conduct or guidance documents are better suited."[104] There is specific concern about how compliance with the regulation will affect small businesses,[105] which is likely the most significant challenge to the

---

[95] ANDREA RENDA ET AL., STUDY TO SUPPORT THE IMPACT ASSESSMENT OF THE AI REGULATORY REQUIREMENTS FOR ARTIFICIAL INTELLIGENCE IN EUROPE 107–08 (2021).

[96] Reid Blackman & Ingrid Vasiliu-Feltes, *The EU's AI Act and How Companies Can Achieve Compliance*, HARV. BUS. REV. (Feb. 22, 2024), https://hbr.org/2024/02/the-eus-ai-act-and-how-companies-can-achieve-compliance [https://perma.cc/3LAX-P44X].

[97] AI Act, *supra* note 9, at ch. XII, art. 99(3).

[98] *Id*.

[99] *Id.* at ch. XII, art. 99(1)–(2).

[100] *See* ANDREA RENDA ET AL., *supra* note 95.

[101] *Id.* at 12, 134.

[102] *Id.* at 12.

[103] *Id.*

[104] *Id.* at 104.

[105] *Id.* at 108.

implementation of a similar system in the United States. Indeed, the United States Chamber of Commerce provided in its stakeholder response to the impact assessment that compliance will limit innovation and growth:

> A new conformity assessment regime would likely serve as a significant bottleneck in the development and deployment of AI in the EU, as companies would need to win approval from regulators before deploying AI-enabled goods and services in the Single Market. Many innovative small and medium-sized enterprises that may have neither the time nor resources to undergo such a process will either avoid investing in perceived "high risk" areas or deploy their solutions abroad. The additional costs will reduce competition and choice in the Single Market for AI goods and services deemed as "high risk."[106]

This response raises the question as to whether the United States may adopt a similar regulatory approach as it attempts to establish laws for the safe and responsible use of AI systems.

III. THE UNITED STATES' APPROACH TO REGULATING AI SYSTEMS

A. Bipartisan Framework for United States Act

In response to the proliferation of unfettered access to unregulated AI systems, a wave of momentum has surged around the development of protective legislation.[107] In 2023, United States Senators Josh Hawley (R-MO) and Richard Blumenthal (D-CT) introduced a "legislative framework to establish guardrails for artificial intelligence[,]" the Bipartisan Framework for U.S. Act ("Bipartisan Framework").[108] The Bipartisan Framework is brief but acts as a proposed roadmap for establishing future AI legislation.[109]

The Bipartisan Framework has five principles:

---

[106] *Id*.

[107] *See Hawley Announces Guiding Principles for Future AI Legislation*, JOSH HAWLEY: U.S. SEN. FOR MO. (June 7, 2023), https://www.hawley.senate.gov/hawley-announces-guiding-principles-future-ai-legislation [https://perma.cc/YQZ3-ACHS]; *Hawley*, *Blumenthal Introduce Bipartisan Legislation to Protect Consumers and Deny AI Companies Section 230 Immunity*, JOSH HAWLEY: U.S. SEN. FOR MO. (June 14, 2023), https://www.hawley.senate.gov/hawley-blumenthal-introduce-bipartisan-legislation-protect-consumers-and-deny-ai-companies-section [https://perma.cc/GV32-VG47].

[108] *Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation*, RICHARD BLUMENTHAL: U.S. SEN. FOR CONN. (Sept. 8, 2023), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-hawley-announce-bipartisan-framework-on-artificial-intelligence-legislation [https://perma.cc/B27D-JAMT].

[109] *Id*.

1. **Establish a licensing system overseen by an independent body:** Providers that develop high-risk products or general-purpose AI systems (large language model AI systems) should be required to obtain a license and register with an "independent oversight body." The licenses would be provided on the condition that providers "maintain[] risk management, [conduct] pre-deployment testing, [have] data governance, and [have] adverse incident reporting programs."

2. **Create legal accountability for injuries**: AI providers should be held liable through enforcement by an oversight body and should be subject to private rights of action when their AI systems subject others to injuries. This provision explicitly calls for general AI systems to be excluded from Section 230 of the Communications and Decency Act.

3. **Ensure the defense of national security and worldwide competitiveness:** Advanced AI systems and hardware should not be transferred to adversarial states, including Russia and China.

4. **Develop transparency requirements**: Providers should be required to disclose "training data, limitations, accuracy, and safety [AI] models to users and companies deploying systems." Additionally, providers should be required to provide notice of interaction with AI systems. AI-generated images and video should be required to maintain a watermark or some other disclosure to notify users of interaction with AI-generated media. A public database should be developed to ensure wide accessibility of potential AI-related harms.

5. **Implement safety measures for consumers and children:** Providers should put users on notice concerning when and how AI is being used. Further, individuals "should have control over how their personal data is used . . . ."[110]

In contrast to the AI Act's hundreds of pages, the Bipartisan Framework's one-page roadmap is not meant to represent a sweeping plan. It is, however, meant to be a hazy reflection of lawmakers' view of the components to be potentially incorporated into a comprehensive United States AI legislative bill. The framework serves as a nod to the EU's AI Act, sharing the attributes of requiring high-risk providers to register with an oversight body,

[110] Sen. Richard Blumenthal & Sen. Josh Hawley, *Bipartisan Framework for U.S. AI Act*, RICHARD BLUMENTHAL: U.S. SEN. FOR CONN. (last visited Mar. 25, 2024), https://www.blumenthal.senate.gov/imo/media/doc/09072023bipartisanaiframework.pdf [https://perma.cc/FQ9J-5WUJ].

transparency and notification of use, and that providers share relevant information about AI systems with interested users.[111]

B. No Section 230 Immunity Act

Section 230 of the Communications Decency Act prohibits liability against internet providers for injuries resulting from third-party content.[112] Section 230 immunity has permitted the internet to proliferate.[113] It has allowed an internet environment—most saliently illustrated by social media platforms—where injuries generated by third-party content creators go unpunished.[114] This led to Section 230 criticism and calls for reform.[115]

In an explicit bid to "[avoid] the same mistakes with generative AI . . . with Big Tech on Section 230," the same Senators introduced a bill entitled "No Section 230 Immunity Act," which as its name suggests, proposes amending Section 230 to allow civil lawsuits and criminal prosecutions relating to generative AI.[116] Senator Ted Cruz objected to this bill proposal on substantive and procedural grounds.[117] With regard to the substantive objection, Senator Cruz pointed to the substantial amount of money—thirty-eight billion dollars in 2023 alone—that has been poured into American AI companies.[118] Senator Cruz emphasized concerns about staying and remaining competitive with other countries, stating "Look, there is a global race for AI, and it is a race we are engaged in with China . . . we need to make sure America is leading the AI revolution."[119] Senator Cruz expresses Big Tech's concerns about reducing America's competitive advantage and squashing innovation.[120]

---

[111] *Id*.; *see generally* AI Act, *supra* note 9.

[112] 47 U.S.C. § 230(c).

[113] Susan P. Crawford, *Shortness of Vision: Regulatory Ambition in the Digital Age*, 74 FORDHAM L. REV. 695, 709 (2005); Nicole Phe, *Social Media Terror: Reevaluating Intermediary Liability Under the Communications Decency Act*, 51 SUFFOLK U. L. REV. 99, 101 (2018).

[114] Alex Chemerinsky & Erwin Chemerinsky, *Misguided Federalism: State Regulation of the Internet and Social Media*, 102 N.C. L. REV. 1, 3 (2023).

[115] *See id*.

[116] S. 1993, 118th Congress (2023–2024); Katie Paul, *Bipartisan U.S. Bill Would End Section 230 Immunity for Generative AI*, REUTERS (June 14, 2023, 12:43 PM), https://www.reuters.com/technology/bipartisan-us-bill-would-end-section-230-immunity-generative-ai-2023-06-14/ [https://perma.cc/P2CD-JN4F].

[117] 169 CONG. REC. S5931-32 (daily ed. Dec. 13, 2023) (statement of Sen. Cruz).

[118] *Id.*

[119] *Id.*

[120] James Czerniawski*, Congress Should not Create Same Altman's Regulatory Moat for AI*, AMS. FOR PROSPERITY (May 17, 2023), https://americansforprosperity.org/why-ai-licensing-proposals-are-bad/ [perma.cc/VSH9-2SB7]; *see generally* Claudia Grisales, *The Who's Who of the Tech World Meet with Senators to Debate Plan to Regulate AI*, NPR (Sept. 13, 2023, 2:32 PM), https://www.npr.org/2023/09/13/11989

Although the proposed Bipartisan Framework and the Section 230 Act illustrate a recognition that the United States must create some comprehensive AI regulatory structure, "lawmakers have struggled to regulate emerging technologies, from the internet to social media . . . ."[121] Despite an understanding that a comprehensive regulatory structure is needed, it is evidence that significant disagreement exists over exactly how to regulate AI.[122]

C. Executive Order 14110 on Safe, Secure, and Trustworthy Artificial Intelligence

The Executive Branch has paid acute attention to establishing AI guidance. Most recently, the Biden Administration issued Executive Order 14110 on Safe, Secure, and Trustworthy Artificial Intelligence ("Executive Order").[123] The Executive Order's purpose is to encourage responsible AI use, increase innovation, and ensure security while limiting societal harms.[124]

The Executive Order takes several significant steps to accomplish its purpose, such as requiring providers to produce the results of their safety tests.[125] A significant portion of the Executive Order instructs government agencies to conduct studies and develop additional guidance on the safe use of AI.[126] The Executive Order directs over fifty agencies to take over 100 "specific actions to implement the guidance," including key policy interests that the Biden Administration has identified, such as "[s]afety and security," "[i]nnovation and competition," "[w]orker support," "[c]onsideration of AI bias and civil rights," "[c]onsumer protection," "privacy," "[f]ederal use of AI," and "[i]nternational leadership."[127]

Working hand in glove with the Executive Office on these matters is the Office of Management and Budget ("OMB"). The OMB issued a proposed memorandum on Advancing Governance, Innovation, and Risk Management

94746/top-tech-leaders-are-to-meet-with-u-s-senators-on-the-future-of-ai-regulation#:~:text=The%20gathering%20is%20part%20of,AI%20policy%20Congress%20can%20pass [https://perma.cc/GXS5-26XN] ("'We should not create a licensing regime for AI,' [IBM CEO Arvind] Krishna is expected to say. 'A licensing agreement would inevitably favor large, well-funded incumbents and limit competition.'").

[121] Grisales, *supra* note 120.

[122] *Id*.

[123] Exec. Order No. 14110, 88 Fed. Reg. 75191 (Nov. 1, 2023).

[124] *Id.* at 75191.

[125] *Id.* at 75197; Will Henshall, *Why Biden's AI Executive Order Only Goes So Far*, TIME (Nov. 1, 2023, 5:55 PM), https://time.com/6330652/biden-ai-order/ [https://perma.cc/M8XJ-2PY4].

[126] Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023).

[127] LAURIE HARRIS & CHRIS JAIKARAN, HIGHLIGHTS OF THE 2023 EXECUTIVE ORDER ON ARTIFICIAL INTELLIGENCE FOR CONGRESS 2 (2023).

for Agency Use of Artificial Intelligence ("OMB Memo").[128] The OMB Memo specifically "direct[s] agencies to advance AI governance and innovation while managing risks from the use of AI . . . particularly those affecting the safety and rights of the public."[129] Pursuant to the Executive Order, the OMB Memo assists the Biden Administration in developing "programs and operations" through the White House Artificial Intelligence Council to facilitate coordination among the various agencies.[130]

Controversially, the Executive Order invokes the Defense Production Act ("DPA") to require providers who have developed or intend to develop "dual-use" generative AI systems to report their model training data, testing data, and data ownership information to the federal government.[131] The DPA also authorizes the Executive Branch to compel action to protect and further national security interests.[132] The DPA, however, is normally invoked only in response to a national emergency.[133]

The Biden Administration posits that invocation of the DPA is appropriate here because AI *does* pose a threat to national security.[134] Some congressional members disagree, arguing that the United States is not experiencing an AI "national emergency."[135] Although the scope of the Executive Order's application under these circumstances is unclear, critics argue that this maneuver is an "executive overreach."[136]

Though these requirements reflect some progress in advancing the creation of laws applicable to AI, enforcing compliance presents more questions than answers, such as the following: What are the Department of Defense's remedies if a company fails to comply with the Executive Order? Will the federal government contract with companies that conduct testing that fail to meet the governments standards? What effect would noncompliance have on these companies' ability to operate within the United States more broadly? The answers to these questions will likely be hard-fought as the Executive Order is challenged in future lawsuits.[137]

---

[128] Memorandum from Shalanda Young, Director of the U.S. Office of Management & Budget, to Heads of Executive Departments & Agencies (Mar. 28, 2024).

[129] *Id.* at 1.

[130] *Id.* at 13.

[131] Exec. Order No. 14110, 88 Fed. Reg. 75191, 75197 (2023).

[132] ALEXNADRA G. NEENAN & KELLEY M. SAYLER, CONG. RSCH. SERV., IN12286, THE AI EXECUTIVE ORDER AND ITS POTENTIAL IMPLICATIONS FOR DOD 2 (2023).

[133] *Id.*

[134] Mohar Chatterjee & Brendan Bordelon, *The Campaign to Take Down the Biden Executive Order*, POLITICO (Jan. 26, 2024, 5:00 AM), https://www.politico.com /news/2024/01/25/conservatives-prepare-attack-on-bidens-ai-order-00137935 [https:/ /perma.cc/M7ZK-MT68].

[135] *Id.*

[136] NEENAN & SAYLER, *supra* note 132, at 2; Chatterjee & Bordelon, *supra* note 134.

[137] Chatterjee & Bordelon, *supra* note 134.

The Executive Order's effect, as applied, is vague.[138] And "[w]hile executive orders are intended to have the force and effect of law, they are not codified in statute."[139] Executive orders are malleable. They are subject to amendment, recension, or revocation—these issues are particularly salient as the 2024 presidential election looms.[140] Because federal laws are not as readily subject to political winds, to create an extensive regulatory scheme with lasting impact, Congress would need to establish laws "reinforcing" the content of the Executive Order.[141] This need points back to questions regarding Congress's willingness to pass comprehensive regulation. At this juncture, at least several congressional members have indicated that they are not supportive of the Executive Order, thus codifying the Executive Order to transform it into a law "with teeth" is unlikely in the present political environment.[142]

AI poses a present and urgent risk. The public is subject to widespread and ubiquitous AI use. For example, consider a hypothetical Jane Doe. While walking to the local mall, Jane is passed by a car driven by an AI system.[143] During Jane's walk, her facial image is captured, stored, and accessed by the city's police department for future use in a photo line-up.[144] Jane's pace and irregular heartbeat are recorded and stored by her smartwatch, which becomes the basis that Jane's health insurance coverage is not renewed.[145] When Jane reaches her destination, she is denied access to credit based on the local department store's algorithmic instructions.[146] The myriad of harms potentially arising from these AI uses, and many others, are largely unregulated. Although developing a comprehensive regulatory structure for AI would present a complicated process requiring bipartisan compromise, given the risks stated above, Congress should endeavor to come to an

---

[138] Henshall, *supra* note 125.

[139] NEENAN & SAYLER, *supra* note 132, at 3.

[140] *See generally id.*

[141] Henshall, *supra* note 125.

[142] Chatterjee & Bordelon, *supra* note 134; *see* Blackman & Vasiliu-Feltes, *supra* note 96.

[143] Stephanie Arnett, *We Need to Focus on the AI Harms that Already Exist*, MIT TECH. REV. (Oct. 30, 2023), https://www.technologyreview.com/2023/10/30/1082656/focus-on-existing-ai-harms/ [https://perma.cc/ZKF8-7VZX]; *see generally* Brian S. Haney, *The Optimal Agent: The Future of Autonomous Vehicles & Liability Theory*, 30 ALB. L.J. SCI. & TECH. 1, 1 (2020).

[144] Arnett, *supra* note 143; *see generally* Valena Beety, *Considering "Machine Testimony": The Impact of Facial Recognition Software on Eyewitness Identifications*, 60 DUQ. L. REV. 271, 277 (2022).

[145] Arnett, *supra* note 143; *see generally* Andis Robeznieks, *Insurers Want Patients to Use Wearables. That Could be a Problem*, AMA (Aug. 26, 2019), https://www.ama-assn.org/print/pdf/node/36421 [https://perma.cc/8JHP-T8D7].

[146] *See* Arnett, *supra* note 143; *see generally* Susan Block-Lieb & Edward J. Janger, *Impact Ipsa Loquitur: A Reverse Hand Rule for Consumer Finance*, 45 CARDOZO L. REV. 1133, 1151 (2024).

agreement to establish a workable framework to protect the American public from the otherwise laissez-faire approach that is present today.

IV. CONCLUSION

The EU's AI Act showcases its twenty-seven-member states' ability to work together to establish a robust and comprehensive regulatory framework like no other. The AI Act's adopted language is hundreds of pages long and considers pragmatic factors, such as creating the AI Office, requiring sandboxes for testing purposes, and requiring red-teaming for certain AI systems. Application of the AI Act will likely present significant compliance challenges and will prove costly. Interested stakeholders have criticized the AI Act on these bases. But the most significant problem with respect to wider replication of the AI Act is the potential impact it and other similar regulatory structures will pose to inhibiting innovation.

Viewing AI research and development as an arms race against other nations raises skepticism among commentators as to whether policymakers will ever establish a similarly sweeping regulatory structure in the United States. Indeed, considering that some have argued that the Executive Order is an overreach because it will "stifle innovation in the AI sector[,]"[147] it is difficult to imagine Congress alone navigating the choppy and uncertain waters of passing a comprehensive federal regulatory system for AI. But passing such a framework would protect the average Jane Doe who may be regularly affected by AI and largely left without recourse when AI errs.

[147] Chatterjee & Bordelon, *supra* note 134.