Emory International Law Review

Volume 37 | Issue 4

2023

Smart Regulation: Lessons from the Artificial Intelligence Act

John Hillman

SMART REGULATION: LESSONS FROM THE ARTIFICIAL INTELLIGENCE ACT

ABSTRACT

The European Union (EU) has recently announced that it will consider a proposal to systematically regulate artificial intelligence (AI) systems. This regulation will add to the legacy of other data regulation acts adopted in the EU and move the EU closer to a comprehensive framework through which it can address rapidly evolving technologies like AI. The United States has yet to implement data regulation or AI regulation legislation at the federal level. This inaction by the United States could negatively impact global cooperation with the EU and China and innovation within the United States. The United States is currently the global leader in AI technology. However, if it wants to maintain that position, it should consider the negative repercussions of dragging its feet regarding regulation. This Comment will demonstrate why systematic regulation of the type being developed in the EU should be adopted in the United States.

TABLE OF CONTENTS

INTRODUCTION

Experts concur that artificial intelligence (AI) will cause fundamental changes that will permeate all aspects of our future lives.[1] AI has famously been defined as simply a computer performing a task that would be considered intelligent if done by a human.[2]

More specifically, AI encompasses three subsets of technology.[3] The first is robotic process automation (RPA), which is the automation of both physical and digital tasks that humans traditionally perform.[4] The second is cognitive insight AI, which uses algorithms to digest data and recognize meaning by detecting patterns.[5] The last category is cognitive engagement AI, which incorporates natural language processing and machine learning.[6] Machine learning is the

---

[1] Darrell M. West & John R. Allen, *How Artificial Intelligence Is Transforming the World*, BROOKINGS (Apr. 24, 2018) ("AI is a technology that is transforming every walk of life. It is a wide-ranging tool that enables people to rethink how we integrate information, analyze data, and use the resulting insights to improve decision making."); NAT'L SCI. & TECH. COUNCIL, COMM. ON TECH., EXEC. OFF. OF THE PRESIDENT, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE (Oct. 2016) (explaining that AI has "opened up new markets and new opportunities for progress in critical areas such as health, education, energy, and the environment" and "[e]xperts forecast that rapid progress in the field of specialized artificial intelligence will continue").

[2] This is a dated, human-centered definition as computer intelligence is much more apt at certain tasks that humans are incapable of performing. However, this is a good starting point for thinking about AI. JOHN ZERILLI WITH JOHN DANAHER ET AL., A CITIZEN'S GUIDE TO ARTIFICIAL INTELLIGENCE 1 (2021).

[3] Thomas H. Davenport & Rajeev Ronanki, *Artificial Intelligence for the Real World*, HARV. BUS. REV., 108–16 (2018), https://hbr.org/2018/01/artificial-intelligence-for-the-real-world (noting that the average citizen or business executive is often confused by the hype surrounding AI, which can manifest in very different forms).

[4] *Id*. ("Tasks include: transferring data from e-mail and call center systems into systems of record; . . . replacing lost credit or ATM cards, reaching into multiple systems to update records and handle customer communications; reconciling failures to charge for services across billing systems by extracting information from multiple document types; and 'reading' legal and contractual documents to extract provisions using natural language processing."); *but see* LAURIE A. HARRIS, CONG. RSCH. SERV., R46795, ARTIFICIAL INTELLIGENCE: BACKGROUND, SELECTED ISSUES, AND POLICY CONSIDERATIONS, 3 (2021) (explaining that some experts argue that RPA should not be classified as AI).

[5] Davenport, *supra* note 3, at 5. ("[U]sed to: predict what a particular customer is likely to buy; identify credit fraud in real time and detect insurance claims fraud; analyze warranty data to identify safety or quality problems in automobiles and other manufactured products; automate personalized targeting of digital ads; and provide insurers with more-accurate and detailed actuarial modeling.").

[6] *Id*. at 6. ("This category includes: intelligent agents that offer 24/7 customer service addressing a broad and growing array of issues from password requests to technical support questions—all in the customer's natural language; internal sites for answering employee questions on topics including IT, employee benefits, and HR policy; product and service recommendation systems for retailers that increase personalization, engagement, and sales—typically including rich language or images; and health treatment recommendation systems that help providers create customized care plans that take into account individual patients' health status and previous treatments.").

class of technology that experts cite as the main driving force behind the coming AI revolution.[7]

It is also important to note the difference between "narrow AI" and "general AI."[8] General AI is what strikes fear into the average citizen; it is the hypothetical sentient, super-intelligent AI predicted to overcome human intelligence.[9] However, that technology is, for now, science fiction.[10] The U.S. Congress, through its research service, has predicted that it will not be realized for at least another decade.[11] Consequently, discussion of AI is typically limited to narrow AI, which is tailored to accomplish a specific, defined task.[12] While this may not immediately lend fodder to the idea of AI's groundbreaking power, narrow AI is already disrupting, one by one, the status quo of each industry it touches.[13] Even RPA, which some argue may not be AI in a strict sense, is a disruptive force in the manufacturing industry.[14]

---

[7] ZERILLI, *supra* note 2, at 3–14 (explaining the different forms of machine learning that "encompass the technologies at the center of the current 'AI revolution'").

[8] HARRIS, *supra* note 4, at 2–3; *see* IBM Cloud Education, *Strong AI*, IBM, (Aug. 31, 2020), https://www.ibm.com/cloud/learn/strong-ai (describing the hypothetical intelligence level that is required for a machine to be considered strong, or general, AI).

[9] HARRIS, *supra* note 4, at 2–3; Ron Schmelzer, *Should We Be Afraid of AI?*, FORBES (Oct. 31, 2019), https://www.forbes.com/sites/cognitiveworld/2019/10/31/should-we-be-afraid-of-ai/?sh=3efdec454331 ("Probably the biggest fear of AI making media waves is that of super intelligence or that AI will reach a point where it doesn't care for or about the existence of humanity anymore, such as what happens with Skynet in the Terminator series of movies.").

[10] HARRIS, *supra* note 4, at 2–3; Ragnar Fjelland, *Why General Artificial Intelligence will not be Realized*, NATURE (June 17, 2020) (explaining that there is an overestimation of the capabilities of AI and that while "development of artificial intelligence for specific purposes [] has been impressive, we have not come much closer to developing artificial general intelligence").

[11] HARRIS, *supra* note 4, at 2–3.

[12] *Id*. at 10; ZERILLI, *supra* note 2, at xvii (explaining that "[e]very major AI in existence today is domain-specific").

[13] *Id*. at 28–30; *see* ROSARIO GIRASA, ARTIFICIAL INTELLIGENCE AS A DISRUPTIVE TECHNOLOGY: ECONOMIC TRANSFORMATION AND GOVERNMENT REGULATION 3–4, 24–59 (2020) (describing AI's role in the current "Fourth Industrial Revolution" and the vast number of fields applying AI, including: health care, robots and robotics, autonomous vehicles, worker safety, energy and energy management, banking, speech (voice) recognition, employment, workplace environment and human resources, marketing, search engines, image recognition, entertainment and consumer usages, law firms, accounting, military and national security, government, sports, prediction by businesses); *see also* Melanie Mitchell, *Artificial Intelligence Hits the Barrier of Meaning*, N.Y. TIMES (Nov. 5, 2018), https://www.nytimes.com/2018/11/05/opinion/artificial-intelligence-machine-learning.html (explaining that AI systems are causing issues when implemented if they are not adequately robust).

[14] HARRIS, *supra* note 4, at 10, 28–30.

By 2030, AI is predicted to potentially "deliver additional global economic activity of around $13 trillion."[15] At that time, seventy percent of all companies are expected to have adopted at least some AI technology.[16] AI will work in tandem with other technologies to transform the way humans live in what has been dubbed the "Fourth Industrial Revolution."[17] The "internet of things", the metaverse, autonomous vehicles, 5G, augmented reality, blockchain, and AI are thought to be convergent technologies that together will have an even greater impact than each technology assessed individually.[18] As the world continues to digitize all aspects of our lives through sensors, creating an interconnectedness of new sources of data in digital space, AI will only grow more powerful.[19] While AI may not replace all need for human intelligence, especially in occupations that require "the exercis[e] of judgment, deep creativity in technology and strategy development, and subtle and sophisticated tacit knowledge of how to orient oneself in the social and physical world," AI could serve as a complement to human intelligence in many occupations performed today.[20] In those occupations that survive the Fourth Industrial Revolution, the enhanced productivity that AI will provide will further reduce the need for human labor.[21] Mass unemployment is a likely result, but freedom from work is not necessarily an undesirable outcome.[22] The subsequent relief from many forms of scarcity could, assuming this technology is properly implemented for the good of mankind, result in a world "redolent of Keynes's and Marx's" utopias.[23]

---

[15] Han-Wei Liu & Ching-Fu Lin, *Artificial Intelligence and Global Trade Governance: A Pluralist Agenda*, 61 HARV. INT'L L.J. 407, 408 (2020) (citing Jacques Bughin et al., *Notes from the AI frontier: Modeling the Impact of AI on the World Economy*, MCKINSEY GLOB. INST. (Sept. 2018), https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy).

[16] Bughin, *supra* note 15.

[17] *See* Kimberly A. Houser & Anjanette H. Raymond, *It Is Time to Move Beyond The 'AI Race' Narrative: Why Investment and International Cooperation Must Win the Day*, 18 NW. J. TECH. & INTELL. PROP. 129, 130 (Mar. 2021) (describing Klaus Schwab's theory of the Fourth Industrial Revolution).

[18] NICHOLAS JOHNSON & BRENDAN MARKEY-TOWLER, ECONOMICS OF THE FOURTH INDUSTRIAL REVOLUTION: INTERNET, ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN 5 (2021).

[19] *See id*. at 115 ("From a technical standpoint, this was made possible by the development of improved machine learning and prediction algorithms to forecast contingencies before they eventuate; the [commercialization] of affordable, lightweight computing hardware with sufficient power for use in new micro-robotics applications; and the development of improved sensory systems to interact with complex operational environments.").

[20] *Id*. at 101–104, 109 (explaining occupations where machines could and could not replace humans).

[21] *Id*. at 107–109.

[22] *Id*. at 109–111.

[23] *Id.* at 109.

Governments across the world have wrestled with the challenges that AI will bring to society and are still in the early stages of determining how to identify and manage the risks that AI presents. The U.S. government has not released a consensus definition of AI, but in the National Artificial Intelligence Initiative Act of 2020, Congress stated that AI "means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."[24] In the recent EU proposal, *Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts* (Artificial Intelligence Act or AIA), the EU offered a similarly broad definition of AI.[25] While certain subcategories of AI, namely machine learning, may portend more radical changes, the broad categorization taken by both the United States and the EU is appropriate given the wide variety of forms AI can take.[26]

While the United States has issued guidance and white papers on AI's impact on American life, there is "no comprehensive federal legislation on AI in the United States to date."[27] It is true that certain statutes already in effect create liability and grant relief to victims of harmful decisions made using AI.[28] The Federal Trade Commission Act gives the Federal Trade Commission (FTC) general authority to enforce unfair and deceptive trade practices, which encompass some commercial uses of AI.[29] However, the inability of the United

---

[24] Catherine Zhu & Louis Lehot, *United States: Artificial Intelligence Comparative Guide*, MONDAQ (Apr. 21, 2021), https://www.mondaq.com/unitedstates/technology/1059776/artificial-intelligence-comparative-guide (giving a general overview of the current legislative and regulatory schemes in effect in the United States); National Artificial Intelligence Initiative Act of 2020, enacted as part of the William M. (Mac) Thomberry National Defense Authorization Act (NDAA) for Fiscal Year 2021, H.R. 6395, 116th Cong. Div. E (2020).

[25] *Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021) [hereinafter *Artificial Intelligence Act* or *AIA*] (defining artificial intelligence system as a "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 such as content, predictions, recommendations, or decisions influencing the environments they interact with").

[26] HARRIS, *supra* note 4, at 3–4.

[27] Zhu & Lehot, *supra* note 24.

[28] Those acts include the Fair Credit Reporting Act, the Equal Credit Opportunity Act, Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Housing Act, and the Genetic Information and Nondiscrimination Act. *Id.*

[29] *Id.*; Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FED. TRADE COMM'N (Apr. 19, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (instructing companies using AI to "[s]tart with the right [data] foundation," "make sure [their algorithm] doesn't discriminate on the basis of race, gender, or other protected class," "embrace transparency and independence," "[d]on't exaggerate what your algorithm can do or whether it can deliver fair or unbiased results," "[t]ell the truth about how you use data," "[d]o more good than harm," and "hold yourself accountable for your algorithm's performance"); *see also* 15 U.S.C. § 57a.

States to pass comprehensive legislation, just as it has failed to do with data protection legislation, has, in practice, left decisions about AI up to individual states and agencies.[30] The United States has hesitated to regulate its thriving AI industry for fear that regulation will result in the United States falling behind Chinese AI development, resulting in a loss of military supremacy. Ironically, that hesitancy and defense-first mindset may end up causing the U.S. AI industry to stagnate.

In sharp contrast stands the European Union (EU) which, in the wake of the impactful General Data Protection Regulation (GDPR), has recently proposed the AIA, the first comprehensive legislation in the world regulating the use of AI.[31] If the AIA is adopted, the European Commission will attempt to set the international standard for AI regulation as it did with the GDPR. In 2022, a vote is expected on the proposal after it is reviewed and amended, with the possibility of an effective date two years after it is signed.[32] The EU proposal is a risk-based regulatory framework that "bans specific unacceptable uses of AI, heavily regulates some other uses that carry important risks and says nothing—except encouraging the adoption of codes of conduct—about the uses that are of limited risk or no risk at all."[33] The proposal will set a single standard across the EU and will require Member States to comply with enforcement and provide a private right of action to those harmed by AI, all in a similar fashion to the framework established by the GDPR.[34] The United States should learn from the AIA and

---

[30] GIRASA, *supra* note 13, at 97–102 (explaining that one of the issues with the *Safe Ensuring Lives Future Deployment and Research in Vehicle Evolution Act* (Self Drive Act), which died in the Senate in 2018, was the potential preemption of state laws regulating autonomous vehicles that were being considered in at least 33 states); *Legislation Related to Artificial Intelligence*, NAT'L CONF. STATE LEGISLATURES (Sept. 15, 2021) https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx ("General artificial intelligence bills or resolutions were introduced in at least 17 states in 2021, and enacted in Alabama, Colorado, Illinois and Mississippi."); *see* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the U.S. (And Why It Matters)*, N.Y. TIMES WIRECUTTER (Sept. 6, 2021) (explaining the disjointed data privacy laws that exist within the United States); Zhu & Lehot, *supra* note 24 ("The United States does not have a federal privacy law and instead currently has a sectoral model when it comes to privacy.").

[31] Eve Gaumond, *Artificial Intelligence Act: What Is the European Approach for AI?*, LAWFARE (June 4, 2021), https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai; *see also* REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[32] Gaumond, *supra* note 31; *Artificial Intelligence Act*, *supra* note 25, at 6.

[33] Gaumond, *supra* note 31.

[34] *Artificial Intelligence Act*, *supra* note 25, at 6.

seek to implement a federal regulatory system to protect its citizens and streamline innovation.

This article will analyze the various components of the AIA; compare the AIA to the current US system; explore the interplay between AI regulation, data regulation, and global politics; and provide justification for developing a comprehensive, federal regulatory framework for data and AI in the United States. Section I of this Article will provide an overview of the AIA and its regulatory methodology.[35] It will explore the different categories of AI under the AIA and explain the intellectual property considerations not incorporated into the document.[36] Section II will discuss how the United States has approached AI regulation and the motivation driving that approach to policy.[37] Section III will explain how the AIA fits into the larger regulatory scheme governing data in general in the EU.[38] The subsections will address the interplay between the existing GDPR and the importance of a robust regulatory system that includes regulation on data collection as well as the methods of using that data in AI systems.[39] Section IV will discuss the competing data regulatory schemes that have emerged in the United States, the EU, and China and the related global power struggle regarding data collection and AI innovation.[40] Section V will briefly summarize and explain why comprehensive regulation at the federal level for data and AI is important for innovation and the protection of citizens' personal rights in the United States.[41]

I. THE NEW EUROPEAN COMMISSION PROPOSAL

The AIA is self-proclaimed to be a part of a larger regulatory scheme and will work in conjunction with "the Digital Decade . . . the Data Governance Act, the Open Data Directive and other initiatives under the EU strategy for data."[42]

---

[35] *See infra* notes 42–115 and accompanying text.

[36] *Id.*

[37] *See infra* notes 116–66 and accompanying text.

[38] *See infra* notes 167–242 and accompanying text.

[39] *See infra* notes 200–42 and accompanying text.

[40] *See infra* notes 243–325 and accompanying text.

[41] *See infra* notes 326–53 and accompanying text.

[42] *Id.* at 5–6 (citing *Communication from the Commission, Shaping Europe's Digital Future*, COM (2020) 67 final (Feb. 19, 2020); *2030 Digital Compass: the European way for the Digital Decade*, COM (2021) 118 final (Mar. 9, 2021); *Proposal for a Regulation on European data governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020); Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-Use of Public Sector Information, 2019 O.J. (L 172) 56–83; *A European strategy for data*, COM (2020) 66 final (Feb. 19, 2020)).

The purpose of this scheme is to establish trustworthy AI and to develop "high quality," transparent AI models.[43] The proposal states that the main areas of regulatory concern are the safety of AI systems, "algorithmic discrimination," and the power of law enforcement.[44] Like the GDPR, the laudatory goals of the proposal arise from the European Union Charter of Fundamental Rights, specifically the right to human dignity; respect for private life and protection of personal data; non-discrimination; equality between women and men; freedom of expression; freedom of assembly; defense and the presumption of innocence; fair and just working conditions; rights of the child; integration of persons with disabilities; and a high level of environmental protection.[45] The proposal also recognizes the growing need for a comprehensive system that will avoid inconsistent AI laws in the EU, which would hinder the development of AI by "fragment[ing]" the market.[46] While the proposal establishes rigid categories of AI applications, it aspires to create a fluid framework that can adapt to every AI system and can endure even as technology progresses.[47] The creation of entities with oversight and reporting responsibilities within each Member State and the establishment of an overarching European Artificial Intelligence Board comprise the structured enforcement body that holds the power to promulgate standards in Member States.[48] The regulatory system creates three categories of

---

[43] *Artificial Intelligence Act*, *supra* note 25, at 5.

[44] *Id*. at 4–5.

[45] *Id*. at 11; *see* GDPR, *supra* note 31, at 1; Charter of Fundamental Rights of The European Union arts. 1, 7–8, 11–12, 21, 23–24, 26, 28, 31, 37, 47–48, 2012 O.J. (C 326) 391.

[46] It is important to draw the analogy between the federalist structure of the Member States of the EU and the states in the United States. The reliance on state regulation could lead to a similar situation in the United States, where AI markets would be fragmented due to potentially conflicting state laws. *Id*. at 9–10; *see* Peter Cihon, Matthijs M. Maas & Luke Kemp, *Fragmentation and the Future: Investigating Architectures for International AI Governance*, GLOB. POL'Y, Nov. 2020, at 545 (suggesting that global fragmentation can be bad for efficiency of innovation and that "[s]ecretariats of emerging AI initiatives, for example, the OECD AI Policy Observatory, Global Partnership on AI, the UN High-level Panel on Digital Cooperation, and the UN System Chief Executives Board (CEB) should coordinate to halt and reduce further regime fragmentation" for AI regulatory systems, but care should be taken when creating a centralized system as "locking-in an inadequate structure may pose a fate worse than fragmentation").

[47] *Artificial Intelligence Act*, *supra* note 25, at 3.

[48] *Id*. at 15, 35, 72–73. This enforcement model is based on the structure of the GDPR enforcement bodies, and "the European Union seems to want to replicate the same kind of regulatory influence it achieved with the GDPR." Gaumond, *supra* note 31. The GDPR regulatory scheme has run into issues of inconsistency between Member States, mostly attributable to the limited resources of some countries as compared to the tech giants they are attempting to regulate. Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. STRATEGIC & INT'L STUD.: STRATEGIC TECHS. BLOG (Sept. 13, 2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement. Despite those inconsistencies, certain regulatory trends are coalescing. Natalie Farmer, Louie Ka Chun, *Ready to Pounce: Regulators Are Intensifying GDPR Enforcement*, CLEARY GOTTLIEB STEEN & HAMILTON (Feb. 26, 2021), https://www.clearycyberwatch.com/2021/02/ready-to-pounce-regulators-are-intensifying-gdpr-enforcement/.

AI based on application and market: prohibited AI, high-risk AI, and other AI (minimal-risk AI).[49] Those categories are explained further in the following sections.

A. Prohibited AI

Prohibited AI practices are laid out in Article 5 of the AIA.[50] The proposal prohibits any AI that uses subliminal techniques to manipulate individuals, exploits vulnerabilities of any specific group, allows public authorities to evaluate or classify the "trustworthiness of natural persons over a certain period of time based on their social [behavior] or known or predicted personal or personality characteristics" (i.e., social score), or uses "'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement."[51] There are exceptions for the use of real-time biometrics, including: "targeted search for specific potential victims of crime, including missing children," substantial or imminent threats involving terrorists, and "detection, [localization], identification or prosecution of a perpetrator or suspect of a criminal offence" that has "a maximum period of at least three years, as determined by the law of [the relevant] Member State."[52] The proposal also

---

[49] *Artificial Intelligence Act*, *supra* note 25, at 12–15; *see* Gaumond, *supra* note 31 ("Balancing the preservation of individual safety and fundamental rights without overly inhibiting innovation in AI is difficult. The AI Act has attempted to find the middle ground by adopting a risk-based approach that bans specific unacceptable uses of AI, heavily regulates some other uses that carry important risks, and says nothing—except encouraging the adoption of codes of conduct—about the uses that are of limited risk or no risk at all.").

[50] *Artificial Intelligence Act*, *supra* note 25, at 43–46.

[51] *Id*. The social score provisions seem to be a direct response to and denouncement of the social scoring program currently being implemented in China. Gaumond, *supra* note 31; s*ee* MICHAEL D. SUTHERLAND, CONG. RSCH. SERV., IF11342 – VERSION: 6, CHINA'S CORPORATE SOCIAL CREDIT SYSTEM (updated Jan. 17, 2020) ("In July 2019, the State Council issued Guiding Opinions on *Accelerating the Building of the Social Credit System*, which urges government agencies to 'fully employ next-generation information technologies such as big data and artificial intelligence to achieve comprehensive credit monitoring.'").

[52] *Artificial Intelligence Act*, *supra* note 25, at 44. Real-time facial recognition technology is already being implemented in law enforcement applications outside of these uses in the United States. One software, Clearview, was adopted by "more than 600 law enforcement agencies" in 2019 and enables users to "potentially be able to identify every person they s[ee]" in real-time. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020) ("Federal and state law enforcement officers said that while they had only limited knowledge of how Clearview works and who is behind it, they had used its app to help solve shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases."). Police forces in major cities have taken notice of the uses of real-time biometrics and have recommended best practices associated with the use of the technology. THE MAJOR CITIES CHIEFS ASS'N, FACIAL RECOGNITION TECHNOLOGY IN MODERN POLICING – RECOMMENDATIONS AND CONSIDERATIONS (Oct. 13, 2021). *See also* KELSEY Y. SANTAMARIA, CONG. RSCH. SERV, R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS, 7–10 (Sept. 24, 2020) (stating that "[t]o date, there is no federal framework specifically directed at the use of FRT by government and private entities[, b]ut some

gives factors to consider for determining if real-time biometric use is appropriate for a given situation, which include the nature of the situation giving rise to its use and the subsequent impact on the rights of persons affected.[53]

B. High-Risk AI

High-risk AI includes, by default, biometric identification and categorization of natural persons, management and operation of critical infrastructure, use in education and vocational training, use in employment, workers management and access to self-employment, access to and enjoyment of essential private services and public services and benefits, use in law enforcement, use in migration, asylum and border control management, and use in the administration of justice and democratic processes.[54] In addition, the proposal states that an AI system "shall be considered high-risk where . . . the AI system is intended to be used as a safety component."[55] A detailed list of high-risk AI systems is included in the AIA's Annex.[56] Creators of high-risk AI systems are required to develop a risk

federal laws of general applicability that address the use of biometrics in particular contexts may be relevant," including the Driver's Privacy Protection Act, the Children's Online Privacy Protection Act, and Section 5 of the Federal Trade Commission Act). "FRT platforms have the capability of being used as a surveillance tool by identifying persons in real-time using video feeds layered with FRT technology. Known instances of this type of use of FRT can be found in foreign nations and among certain private sector businesses. MCCA best practices for law enforcement agencies utilizing FRT is to not utilize FRT in this manner except under the most exigent of circumstances or when explicitly permitted under legal authority (e.g., court order)." *Id*.

[53] Specifically, the proposal suggests considering "the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system" and "the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences." *Artificial Intelligence Act*, *supra* note 25, at 44. In the UK, the Surveillance Camera Code of Practice, issued by authority of section 30 of the Protection of Freedoms Act 2012, was recently updated and presented to Parliament following "particular Data Protection legislation, and the judgment in Bridges v South Wales Police." Surveillance Camera Code of Practice, Gov. U.K., https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice (last visited Oct. 22, 2021). The updated code specifically addresses biometric data and leaves open the possibility of its use in real-time by law enforcement. Sec'y of State, Surveillance Camera Comm'r, Surveillance Camera Code of Practice, UK Gov. (June 2013, Amended 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010815/Surveillance_Camera_Code_of_Practice__update_.pdf.

[54] *Artificial Intelligence Act*, *supra* note 25, at Annex III, pages 4–5.

[55] *Id.*; *see* Simen Eldevik, AI + Safety: Safety Implications for Artificial Intelligence, DNV GL: GRP. TECH. & RSCH. (Aug. 28, 2018), https://ai-and-safety.dnvgl.com/#sec-learn (identifying that "sensor data and data-driven models will become integral to many safety-critical or high-risk engineering systems in the near future" and "data-driven models alone may not be sufficient to ensure safety as usually we do not have exhaustive and fully relevant data").

[56] Notably, the Annex lists in part: "AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons," "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale

management system, establish testing procedures, and maintain up-to-date technical documentation, logging capabilities that records AI activity, transparency of information that allows users to interpret output, and human oversight while the system is in use.[57] The proposal also sets out specific individual obligations for providers, manufacturers, importers, distributors, users, and third parties.[58]

High-risk systems will be the subject of strict oversight by the European Commission.[59] To ensure compliance with the Regulation, EU Member States are required to establish a notifying authority for "setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring."[60] The proposal allows the European Commission to set "common normative standards for all high-risk AI systems" as it sees fit after the proposal is adopted.[61] Member States will develop certificates to be issued to AI systems that they have deemed to conform to the Commission's standards.[62] The proposal also explains how to appeal decisions of non-compliance; how the EU will issue declarations of conformity;

providers for their own use," "AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid," "AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons," and "AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts." *Artificial Intelligence Act*, *supra* note 25, at Annex III, pages 4–5.

[57] *Id.* at 46–47, 49–52.

[58] Providers must ensure compliance, "draw-up the technical documentation," "ensure that the high-risk AI system undergoes the relevant conformity assessment procedure," and "inform the national competent authorities of the Member States in which they made the AI system available." *Id*. at 52–58. Product manufacturers "shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider." *Id*. at 55. Importers must "ensure that (a) the appropriate conformity assessment procedure has been carried out by the provider of that AI system, (b) the provider has drawn up the technical documentation in accordance with Annex IV; (c) the system bears the required conformity marking and is accompanied by the required documentation and instructions of use." *Id.* at 56. Distributors are subject to the same obligations as providers when "(a) they place on the market or put into service a high-risk AI system under their name or trademark; (b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service; (c) they make a substantial modification to the high-risk AI system." *Id*. at 57. Users are required to ensure that obligations are met by the system, to "monitor the operation of the high-risk AI system on the basis of the instructions of use," and "to carry out a data protection impact assessment under Article 35 of [the GDPR] or Article 27 of Directive (EU) 2016/680 [concerning the free movement of data], where applicable." *Id*. at 58.

[59] *Id*. at 58–63.

[60] *Id*. at 58.

[61] *Id*. at 20. The commission is required to consult "relevant bodies or expert groups" when making common specifications. *Id*. 63–65.

[62] "Certificates shall be valid for the period they indicate, which shall not exceed five years," and the certificates can be withdrawn or suspended. *Id*. at 65–66.

the guidelines for marking products as conforming; the requirements for document retention; registration requirements for an EU AI database; and transparency requirements for high-risk AI systems.[63] The proposal also includes recommendations for the creation of "AI sandboxes" in Member States, which are intended to allow companies to test their AI systems for conformity before they are released to the public and to counteract the disincentivizing aspects of AI regulation.[64] This crucial aspect of the Regulation will ensure continued innovation in AI in the EU if the proposal is adopted.[65]

C. Other AI and Enforcement

The third regulatory category encompasses any remaining applications of AI systems, which the proposal deems to be of minimal risk.[66] Article 52 establishes specific transparency requirements for some of these systems, but otherwise, the proposal does not explicitly establish regulatory requirements for these other forms of AI.[67] However, the proposal tasks the European Commission and the

---

[63] *Id.* at 66–69 (stating that "Member States shall ensure that an appeal procedure against decisions of the notified bodies is available to parties having a legitimate interest in that decision" and "[t]he CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems").

[64] *Id.* at 69–71. "AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan." *Id.* at 69. "Participants in the AI regulatory sandbox shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result from the experimentation taking place in the sandbox." *Id.* at 70.

[65] S*ee* Mark Fenwick, Wulf A. Kaal & Erik P. M. Vermeulen, *Regulation Tomorrow: What Happens When Technology Is Faster than the Law*, 6 AM. U. BUS. L. REV. 561, 591–93 (2017) ("In April 2016, the [Financial Conduct Authority] broke new ground by announcing the introduction of a 'regulatory sandbox,' which allows both startups and established companies to roll out and test new ideas, products, and business models in the area of Fintech (i.e., new technologies aimed at making financial services, ranging from online lending to digital currencies, more efficient). The investment data suggests that the UK regulator is moving in the right direction with this kind of decision []. The idea behind the sandbox is to provide a safe space for testing innovative products and services without being forced to comply with the applicable set of rules and regulations. With the sandbox, the regulator aims to foster innovation by lowering regulatory barriers and costs for testing disruptive innovative technologies, while ensuring that consumers will not be negatively affected.") (citations omitted).

[66] *Artificial Intelligence Act*, *supra* note 25, at 80–81; *see* Gaumond, *supra* note 31 ("The defining characteristic of AI systems that fall into this category is that they raise certain issues in terms of transparency and thus require special disclosure obligations. There are three types of technologies that require such special transparency requirements: deep fakes, AI systems that are intended to interact with people, and AI-powered emotion recognition systems/biometric categorization systems.").

[67] *See Artificial Intelligence Act*, *supra* note 25, at 69; Wolfgang A. Maschek et al. *The Proposed New EU Regulatory Regime for Artificial Intelligence (AI)*, SQUIRE PATTON BOGGS (Sept. 2021) ("Certain AI systems will only be subject to new transparency requirements (Title IV), for instance, where there is a risk of manipulation (e.g. chatbots) or deceit (e.g. deep fakes).").

European Artificial Intelligence Board with developing codes of conduct that will apply to these AI systems.[68]

The proposal establishes sanctions and enforcement mechanisms that mirror those created by the GDPR.[69] There are specific penalties for failure to meet the standards in any of the above categories, including: "administrative fines of up to 30 000 000 EUR or, if the offender is a company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher" for non-compliance with AI prohibitions or data governance requirements, and "administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher" for "non-compliance of the AI system with any requirements or obligations under this Regulation."[70] Additionally, supplying "incorrect, incomplete or misleading information" to any oversight authority is "subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher."[71]

D. Missing Intellectual Property Considerations

Interestingly, although the AIA attempts to be a comprehensive regulatory scheme, it fails to address issues that AI will create within the EU's patent

---

[68] *Artificial Intelligence Act*, *supra* note 25, at 80. This section contains a requirement that "[t]he Commission and the Board [] take into account the specific interests and needs of the small-scale providers and start-ups when encouraging and facilitating the drawing up of codes of conduct." *Id.* at 81. Providing start-ups the ability to influence what regulations will be imposed regarding non-high-risk applications could avoid issues of the anticompetitive repercussions of added regulatory hoops. *See* James Bessen et al., *GDPR and the Importance of Data to AI Startups*, N.Y.U. STERN SCH. OF BUS., 18 (Apr. 15, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3576714 ("Though GDPR drives changes that are important to safeguarding personally identifiable information, there are also costs associated with this increased regulation. These startups are reallocating their limited resources and creating new positions to deal with the implications of this regulation. Given that more than 65% of firms included in the survey have fewer than 50 employees, hiring and resource shuffling could be detrimental to longer term success.").

[69] *Artificial Intelligence Act*, *supra* note 25, at 82–83; *see* GDPR, *supra* note 31 art. 83; Mark MacCarthy & Kenneth Propp, *Machines learn that Brussels Writes the rules: The EU's new AI regulation*, BROOKINGS: TECHTANK (May 4, 2021), https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/ ("the European Commission has presented potential penalties of eye-catching severity, even beyond those of the General Data Protection Regulation"); *but see* Jane Wakefield, *Europe Seeks to Limit Use of AI in Society*, BBC: TECH (Apr. 14, 2021), https://www.bbc.com/news/technology-56745730 ("And any companies that develop prohibited services, or fail to supply correct information about them, could face fines of up to 4% of their global revenue, similar to fines for GDPR breaches.").

[70] *Artificial Intelligence Act*, *supra* note 25, at 82–83.

[71] *Id.*

system.[72] Intellectual property is mentioned in Article 70, but only in the context of protecting confidentiality during mandatory disclosures of information and data to regulators.[73] However, the idea that current intellectual property law is robust enough to handle the difficulties presented by AI creations is in question.[74] Issues of patentability undeniably impact innovation.[75] There are several unanswered questions surrounding AI's role in intellectual property that could have been addressed in the AIA.[76]

How should AI systems be protected?[77] AI systems are a software-based subfield of computer science.[78] While general rules about the protection of software, from a subject matter perspective, are being developed in the courts and through USPTO guidance, there are certain specialized reasons for favoring the protection of AI systems through patents.[79] Software is patentable in the United States; however, there must be an additional inventive concept beyond the simple code that makes up the software.[80] Trade secret protection has become the norm for protecting software-based IP in the United States and the

---

[72] *See* Gabriele Engels, *EU Artificial Intelligence Act and IP Rights*, DLA PIPER (Oct. 21, 2021), https://mse.dlapiper.com/post/102h8z0/eu-artificial-intelligence-act-and-ip-rights ("With the drafting of the 'Artificial Intelligence Act' (April 2021), the European Commission has made its first attempt at comprehensively regulating the expansive world of AI. Whilst the draft legislation extensively addresses the regulation and classification of AI technology, it does not mention another area of concern regarding Artificial Intelligence, namely intellectual property rights.").

[73] *See id.*; *Artificial Intelligence Act*, *supra* note 25, art. 70(1)(a).

[74] *See* Engels, *supra* note 72; *see also* Frank A. DeCosta III, Ph.D. & Aliza G. Carrano, *Intellectual Property Protection for Artificial Intelligence*, WESTLAW J. INTELL. PROP. (Aug. 30, 2017), https://www.finnegan.com/en/insights/articles/intellectual-property-protection-for-artificial-intelligence.html (identifying disclosures related to trade secrets and patent-eligible subject matter considerations as areas of uncertainty surrounding intellectual property protection of AI).

[75] *See* Andrea Moriggi, *The Role of Intellectual Property in the Intelligence Explosion*, 4IP COUNCIL 5–6 (2017), https://www.4ipcouncil.com/application/files/9615/1638/1031/The_Role_of_Intellectual_Property_in_the_Intelligence_Explosion.pdf ("Software patents are increasingly deemed a business asset of pivotal importance in the growing software industry; consequently, the predictability of its protection under patent law plays a primary role in investment decisions and, accordingly, on long-term business success.").

[76] *See generally* Jordan R. Jaffe et al., *The Rising Importance of Trade Secret Protection for AI-Related Intellectual Property*, QUINN EMANUEL (2020), https://www.quinnemanuel.com/media/wi2pks2s/the-rising-importance-of-trade-secret-protection-for-ai-related-intellec.pdf.

[77] *Id.*; *see generally* Nicholas James Stamatis, *Patenting Artificial Intelligence: An Administrative Look into the Future of Patent Law*, 19 J. HIGH TECH. L. 329 (2019).

[78] Stamatis, *supra* note 77, at 332.

[79] *Id.* at 336–44.

[80] *Id.* at 338–44; *see* Mayo Collaborative Servs. v. Prometheus Lab'ys, 566 U.S. 66, 72–73 (2012) (explaining that an invention must possess an inventive concept to be patentable); Alice v. CLS Bank Int'l, 573 U.S. 208, 217–27 (2014) (holding that an invention must "do more than simply instruct the practitioner to implement the abstract idea of intermediated settlement on a generic computer").

EU.[81] Trade secret protection may seem more appropriate given the rate of invention in the field of AI, but there are reasons to consider patent protection.[82] There are drawbacks to be considered by inventors opting to keep software secret, specifically reverse engineering and independent inventorship.[83] Ordinarily, the ability to reverse engineer a trade secret provides a much needed check on the otherwise limitless exclusivity offered by trade secret protection.[84] However, AI—and other personal information-based innovations—are exceptionally difficult to reverse engineer than other forms of software.[85] The "black box" nature of many AI systems makes reverse engineering nearly impossible.[86] Therefore, a trade secret may offer far greater protection than intended or presumed by the present law.[87] Additionally, trade secret protection is also justified as a reward for the cost of acquiring the information.[88] But, for many of the datasets used to train AI, the upfront cost is minimal.[89] The AIA fails to address this nuance regarding AI technology and overlooks the opportunity to limit what may be overprotection of AI software within the current intellectual property framework.[90]

Is it fair to allow inventors to claim the fruits of the inventions of AI systems?[91] Currently, the EU does allow patents on computer-implemented

---

[81] Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 YALE J. L. & TECH. 256, 299 (2020).

[82] *See* Jaffe, *supra* note 76, at 6 ("AI technology is rapidly developing and improving at a rate the patent system is not designed to keep up with.").

[83] *See id*. at 7 ("Keeping software a 'secret' can be challenging and operationally taxing for several reasons: (1) given the turnover at technology companies, strong employment agreements are needed to ensure departing employees are legally required to keep trade secrets secret; (2) given the ease of "stealing" software—which can be as easy as downloading code to a USB drive—strong cybersecurity policies need to be created and enforced; (3) because reverse engineering can be a defense to trade secret appropriation, software needs to be designed and deployed in a way to ensure reverse engineering is not possible; and (4) in order to conduct business, it is often necessary to share technology widely with employees and partners, which increases the risk that a trade secret could be disclosed publicly.").

[84] Lev-Aretz & Strandburg, *supra* note 81, at 299–302.

[85] *Id*. at 297–302.

[86] *Id*.

[87] *Id*.

[88] *Id*. at 301 ("From a free rider perspective, trade secrecy is important primarily for recouping the additional upfront costs of amassing personal information. For many personal information-based companies, however, those costs are extremely low, since they acquire personal information as a cheap by-product of providing other products and services.").

[89] *Id*.

[90] *Id.*; s*ee* Engels, *supra* note 72.

[91] The European Patent Office Legal Board of Appeal has stated in a preliminary opinion that "the inventor must be a person having legal capacity." *Artificial intelligence*, EUROPEAN PAT. OFF., https://www.epo.org/news-events/in-focus/ict/artificial-intelligence.html (last visited Jan. 7, 2022); *see also* W.

inventions, but there are unanswered questions about how much disclosure of the working mechanisms of the AI system is necessary to obtain a patent.[92] Additionally, there are economic inequality considerations if AI systems are allowed to gain a foothold in the patent space.[93] AI systems will undoubtedly increase the overall rate of invention because they inherently save time and reduce required labor.[94] The "Distribution Effect" of patent rights is likely to be exacerbated by the assistance of AI in creating inventions.[95] The Distribution Effect recognizes that "intellectual property magnifies the division of rewards between generators of intellectual property and the workers whom their innovations replace."[96] Theoretically, the more patents that inventors can generate, the more monetary rewards those inventors receive to the detriment of those replaced by the invention.[97] While this reasoning always holds true when labor saving inventions are introduced, dramatically increasing the rate of invention could make this an exponentially larger issue.[98] Regardless of the implications of AI inventors, the exclusion of this consideration will result in the European Patent Office developing its own policy independently of European policymakers and the AIA, which may lead to inconsistencies with the goals of promoting innovation.[99]

Michael Schuster, *Artificial Intelligence and Patent Ownership*, 75 WASH. & LEE L. REV. 1945 (2018) (explaining the issues surrounding patenting inventions created solely by AI); *but see* Moriggi, *supra* note 75, at 9 ("However, the fact that the release of independently generated AI creative works falls into the public domain is leaving the academic community divided and some, on the contrary, believe that it would limit innovation, as a result of the impossibility for companies that have invested into the creation of AI machines to enjoy protection or the financial benefits associated with it, eventually dissuading them from investing").

92 *See Patenting Artificial Intelligence and Machine Learning Innovations in Europe*, JONES DAY (Oct. 2018), https://www.jonesday.com/en/insights/2018/10/patenting-artificial-intelligence-and-machine-lear; *see generally* Charlotte A. Tschider, *Beyond the "Black Box,"* 98 DENV. L. REV. 683 (2021).

93 Camilla A. Hrdy, *Intellectual Property and the End of Work*, 71 FLA. L. REV. 303, 333–38 (2019); s*ee also* Jack Kelly, *Artificial Intelligence Has Caused A 50% To 70% Decrease In Wages—Creating Income Inequality And Threatening Millions Of Jobs*, FORBES (June 18, 2021), https://www.forbes.com/sites/jackkelly/2021/06/18/artificial-intelligence-has-caused—50-to-70-decrease-in-wages-creating-income-inequality-and-threatening-millions-of-jobs/?sh=310d87621009.

94 *See* Daryl Lim, *AI & IP: Innovation & Creativity in an Age of Accelerated Change*, 52 AKRON L. REV. 813, 833–34 (2018) ("The growing role of AI in drug innovation helps prioritize experiments and substantially reduces the necessity for experimental work.").

95 Hrdy, *supra* note 93, at 333–38.

96 *Id*.

97 *See id*.

98 *See id*.

99 *See* Engels, *supra* note 72.

If protections are given to AI inventions, who will reap the benefits of the exclusivity provided by the awarded patents?[100] An AI system can theoretically invent much more quickly than a human and, in turn, diminish the value of pure human innovation.[101] However, allowing protection for AI creations encourages the deployment of resources towards the growth of AI technology because of the monetary incentives that patents provide.[102] By not explicitly offering protections for AI inventions, the EU has left open the possibility that it may lose its technological advantage over countries that do offer those protections.[103]

Tangentially, to what extent should AI be used in determining the administration of intellectual property rights?[104] The European Patent Office (EPO) and the United States Patent Office (USPTO) have both considered the idea of using AI "to enhance the efficiency of the patent grant process in classification and search."[105] While this is an important consideration since it involves a government authority granting a citizen the right to exclude others or other protection over a work or mark, it is arguably not included under the high-risk category.[106] Although it involves the "[a]dministration of justice and democratic processes," only "AI systems intended to assist a judicial authority"

---

[100] *See* Katharine Stephens, *Who Owns an AI-generated Invention*?, BIRD & BIRD (Dec. 2019), https://www.twobirds.com/en/news/articles/2019/global/who-owns-an-ai-generated-invention.

[101] *See* Tom Dines, *A Patent Predicament: Who Owns an AI-generated Invention?*, FIN. TIMES (Oct. 6, 2019), https://www.ft.com/content/84677ec8-be73-11e9-9381-78bab8a70848 ("While the idea of granting intellectual property protections to a machine may seem a niche concern now, it will become more pressing as AI systems invent more routinely. Indeed, it is possible that AI is already generating new ideas but that its role is being concealed because of legal uncertainty, according to Mr Abbott.").

[102] *See id.* ("The problem is that if AI cannot be recognised as an inventor, the owners of the AI will not have any protection for the ideas generated by their work. This may discourage them from pushing further development. Not recognising the AI as an inventor threatens innovation by 'failing to encourage the production of socially valuable inventions', argues Mr Abbott's team.").

[103] *See* Shlomit Yanisky-Ravid & Regina Jin, *Summoning a New Artificial Intelligence Patent Model: In the Age of Pandemic*, MICH. ST. L. REV. 2021 (last revised Sept. 17, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3619069 ("We hold that in order to incentivize the players and encourage investments in creative AI systems (including AI algorithms and AI trained models), AI-made inventions must be patentable. However, as the law stands human inventors are only eligible for patent ownership, therefore, a new model is needed.").

[104] *See generally* W. Keith Robinson, *Artificial Intelligence and Access to the Patent System*, 21 NEV. L.J. 729 (2021) (discussing the dangers of "AI-assisted examination").

[105] *Impact of AI on Patent System Explored at EPO Digital Event*, EUROPEAN PAT. OFF. (Dec. 18, 2020), https://www.epo.org/news-events/news/2020/20201218.html; *USPTO Developing New Artificial Intelligence Capabilities for Examiner Search Tool*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/subscription-center/2021/uspto-developing-new-artificial-intelligence-capabilities-examiner-search (last accessed Feb. 12, 2022); *see also* Dan L. Burk, *Racial Bias in Algorithmic IP*, 106 MINN. L. R. HEADNOTES (forthcoming 2022).

[106] *See Artificial Intelligence Act*, *supra* note 25, at Annex III, pages 4–5.

are explicitly mentioned under that umbrella.[107] This could mean that patentability, as well as copyright and trademark similarity assessed by AI, would be found high-risk when used to answer questions involving IP rights in judicial decisions, while the use of AI in the granting of patents by the patent office would not be included under the high-risk category.[108] While the AIA does still impose restrictions on minimum risk systems, there are reasons for classifying this use of AI as high-risk.[109] It has been recently demonstrated that copyright doctrines and concepts regarding creation, including obviousness, have had a disparate impact on African American and Hispanic applicants.[110] Even properly calibrated AI systems, if used to assess patentability, are likely to amplify and entrench the biases that have resulted in the underrepresentation of minority creators.[111] Patent offices should be concerned about increasing the effect of latent bias that has led to the disparate impact of the patent system's granting of intellectual property rights without first addressing the root of the problem.[112] Moreover, if AI is more involved in the patent granting process, the "illusion of objectivity" may make combatting racial biases more difficult.[113]

While these questions may not be answerable right now without further research, they are all important yet unaddressed questions that the AIA has brushed aside.[114] The United States should take a more proactive approach to AI intellectual property protections to further incentivize the development of AI systems in a manner fair to all.[115]

II. UNITED STATES' APPROACH TO AI REGULATION AND DEVELOPMENT

The below section will lay out any restrictions on AI use in the United States at the federal and state levels. It will also explain what the United States has done to promote the creation and use of AI, and how regulation should mash with the United States' objectives for AI advancement and innovation.

---

107 *Id*.

108 *See id*.

109 *See generally* Burk, *supra* note 105.

110 *Id*. at 4–6.

111 *Id*. at 19–20.

112 *Id.*

113 *Id*.

114 *See* Engels, *supra* note 72.

115 *See* Yanisky-Ravid, *supra* note 103, at 34 ("First, we contend that allowing patenting of AI algorithms, a part of AI creative systems, would incentivize the research on fundamental AI building blocks. Not only does it boost the advancement of AI technology itself, more importantly, it encourages the technological development in various fields, such as medical, engineering, and science.").

A. Current Restrictions on AI Use in the United States

The United States has, so far, taken a less aggressive approach to AI regulation, one that is reminiscent of its stance on data privacy laws.[116] By straying from proposing a national regulatory scheme, the U.S. government has left the question of regulating AI to state legislators and executive agencies such as the FTC.[117] While those approaches are not entirely unimportant to preventing abuses by AI, the stage has been set for a patchwork of laws regarding AI to emerge.[118] This system could lead to added obstacles for AI development and implementation for companies by splitting the market throughout multiple jurisdictions with different or competing laws.[119] However, some research has suggested that implementing a comprehensive scheme could, at least temporarily, redirect resources away from research and development to ensure compliance with new regulations.[120]

---

[116] Zhu & Lehot, *supra* note 24; Gaumond, *supra* note 31; *see* Grzegorz Mazurek & Karolina Małagocka, *Perception of Privacy and Data Protection in the Context of the Development of Artificial Intelligence*, J. MGMT. ANALYTICS (Oct. 2, 2019), https://www.tandfonline.com/doi/pdf/10.1080/23270012.2019.1671243?needAccess=true (explaining that U.S. data privacy policy "has been shaped by a long tradition of self-regulation and small government interventionism"); *but see* AI Index Steering Committee, *AI Index Annual Report*, STAN. UNIV. (Mar. 2021) ("The 116th Congress (January 1, 2019–January 3, 2021) is the most AI-focused congressional session in history. The number of mentions of AI by this Congress in legislation, committee reports, and CRS reports is more than triple that of the 115th Congress. Congressional interest in AI has continued to accelerate in 2020.").

[117] Many states have begun enacting their own legislation regarding "automated decision systems." No state legislation in the United States provides a comprehensive regulatory scheme; they are mostly concerned with the impact of AI on insurance and hiring practices. *Legislation Related to Artificial Intelligence*, NAT'L CONF. STATE LEGISLATURES (Sept. 15, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx.

[118] Zhu & Lehot, *supra* note 24 ("[M]uch of the governing legal framework is through the cross-application of rules and regulations governing traditional disciplines such as product liability, data privacy, intellectual property, discrimination and workplace rights. Self-regulation and standards groups also contribute to the governing framework.").

[119] *See* James Rundle, *Privacy Chiefs Say Patchwork Data Laws Mean Lawyers Must Work Alongside Engineers*, WALL ST. J.: RISK & COMPLIANCE J. (May 5, 2021), https://www.wsj.com/articles/privacy-chiefs-say-patchwork-data-laws-mean-lawyers-must-work-alongside-engineers-11620254075 ("Ensuring compliance with data protection laws has become so complicated that companies must make room for regulatory and ethics experts in product engineering processes, privacy executives say."); Kaveh Waddell & Kia Kokalitcheva, *States are Sewing a Patchwork of AV Regulations*, AXIOS (Oct. 27, 2018) ("'You should be able to buy a [autonomous] car in California and drive it to New York,' . . . the National Highway Traffic Safety Administration is best equipped to do this."); *Autonomous Vehicle Laws*, INS. INST. HIGHWAY SAFETY, https://www.iihs.org/topics/advanced-driver-assistance/autonomous-vehicle-laws (updated Oct. 2021).

[120] *See* Bessen et al., *supra* note 68, at 18.

The United States has made some attempts to form a national policy regarding AI at least with regard to its use by the federal government.[121] In February 2019, President Trump released an executive order establishing the American AI Initiative (E.O. 13859).[122] "The E.O. establishe[d] a common set of principles for the design, development, acquisition, and use of AI in the federal government to foster public trust and confidence, and directs the Office of Management and Budget (OMB) to develop policy guidance for implementing the principles across agencies."[123] E.O. 13859 further includes direction to federal agencies.[124] It requires them "to provide annual, publicly-available inventories of nonclassified, nonsensitive use cases of AI," and "undertake activities to expand the number of AI experts at federal agencies," such as creating an "AI track within the Presidential Innovation Fellows program" and by forming new AI educational programs.[125]

Despite this effort, AI innovators and members of Congress worry that the government lacks the expertise to properly address the issues surrounding AI.[126] E.O. 13859 not only sought to expand the knowledge of federal employees for regulatory purposes but also to enable those employees to act as advisors for developing plans regarding the growth of AI technology.[127]

Since E.O. 13859, there have been additional attempts by Congress and agencies to develop AI policies in sector-specific applications.[128] The National

---

121 HARRIS, *supra* note 4, at 16–27.

122 Exec. Order No. 13,859, 84 Fed. Reg. 3967 (Feb. 11, 2019).

123 HARRIS, *supra* note 4, at 17; *see* Russell Vought, *Guidance for Regulation of Artificial Intelligence Applications*, 3–7 (Nov. 17, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf ("Promoting innovation and growth of AI is a high priority of the U.S. government. Fostering AI innovation and growth through forbearing from new regulation may be appropriate in some cases.").

124 HARRIS, *supra* note 4, at 17.

125 *Id*.

126 *Id*. at 30–35; *see* Ryan Tracy, *How Can Government Attract the AI Talent It Needs?*, WALL ST. J. (Apr. 6, 2021), https://www.wsj.com/articles/how-can-government-attract-the-ai-talent-it-needs-11617724802 ("Based on survey responses, the number of AI PhD graduates in the U.S. and Canada has risen in recent years, but the percentage who go to work for the government remains tiny."); Bianca Datta, *Can Government Keep Up with Artificial Intelligence?*, PBS: NOVA (Aug. 10, 2017), https://www.pbs.org/wgbh/nova/article/ai-government-policy/ ("'Expertise is absolutely the first step,' . . . [w]ithout it, 'the government has to rely on other stakeholders, and those stakeholders will have their own interests. Sometimes, if the government doesn't have adequate expertise, it won't act because it will be paralyzed. And other times they will take industry's word for something and act too quickly—and then have a problem.'").

127 HARRIS, *supra* note 4, at 17.

128 *Id*. at 19–27; *see, e.g.*, EPA Plan - Response to OMB's M-21-06 Guidance for Regulation of Artificial Intelligence Applications, EPA (Aug. 2021), available at https://www.epa.gov/laws-regulations/summary-executive-order-13859-maintaining-american-leadership-artificial ("EPA currently has no planned regulatory activity related to AI. EPA has begun work on AI strategies, beginning with technical architecture and internal

Institute of Standards and Technology released guidance on the development of standards in AI in response to the executive order.[129] The Advancing Innovation to Assist Law Enforcement Act was intended to require the Director of the Financial Crimes Enforcement Network to report on the use of AI and other emerging tech within the Financial Crimes Enforcement Network—among other purposes.[130] However, the Act died in the Senate in 2019.[131] The FTC has distributed guidance on its approach to AI bias focused on deceptive and discriminatory AI.[132] The FTC Guidance encourages transparency and accountability.[133] The AI in Government Act of 2020 asked for guidance on the use of AI, urging a need for identifying best practices.[134] In December 2020, President Trump released an executive order promoting the use of trustworthy AI in the federal government (E.O. 13960). [135]

Traditional tort law in the United States is also ill-equipped to handle the detrimental effects of AI.[136] With AI applications, traditional elements of tort liability are difficult to demonstrate in comparison to actions involving human offenders. Foreseeability is a difficult concept to apply to an AI system.[137] The unpredictability of an AI system is generally what makes it useful; AI is used to go beyond the realm of traditional thinking in a specific industry to gain an edge on the competition. Negligence is also a difficult doctrine to apply to AI.[138] Causation, an element of traditional negligence tort claims, is difficult to prove

governance requirements. Over time, this work will be broadened out to include the higher level principles and approaches described in OMB Memorandum M-21-06, including encouraging innovation and growth of AI within the Agency and as a possible part of its regulatory and non-regulatory programs. EPA will be guided by the principles of public trust and public participation, scientific integrity and information quality, risk assessment and management, consideration of benefits and costs, flexibility, fairness and non-discrimination, disclosure and transparency, safety and security, and interagency cooperation.").

129 U.S. DEPT. OF COM., NAT. INST. OF STANDARDS & TECH., U.S. LEADERSHIP IN AI: A PLAN FOR FEDERAL ENGAGEMENT IN DEVELOPING TECHNICAL STANDARDS AND RELATED TOOLS (Aug. 9, 2019), available at https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

130 Advancing Innovation to Assist Law Enforcement Act, H.R. 2613, 116th Cong. (2019).

131 *U.S. Congress HR2613, Advancing Innovation to Assist Law Enforcement Act*, TRACKBILL, https://trackbill.com/bill/us-congress-house-bill-2613-advancing-innovation-to-assist-law-enforcement-act/1748157/.

132 Jillson, *supra* note 29.

133 *Id.*; *see Hearings on Competition and Consumer Protection in the 21st Century*, FED. TRADE COMM'N, https://www.ftc.gov/policy/hearings-competition-consumer-protection (last visited Oct. 23, 2021).

134 AI in Government Act of 2020 incorporated in the Consolidated Appropriations Act, 2021, Pub. L. No. 116–260, 134 Stat. 1182 (2020).

135 Exec. Order No. 13,960, 85 Fed. Reg. 78939 (Dec. 3, 2020).

136 Stefan Heiss, *Towards Optimal Liability for Artificial Intelligence: Lessons from the European Union's Proposals of 2020*, 12 HASTINGS SCI. & TECH. L.J. 186, 199–206 (2021).

137 *Id.*

138 *Id.*

with AI systems, as it can be difficult to establish that harms resulting from the use of AI are the fault of the conduct of the AI system's user.[139] Additionally, it is arguable whether product liability standards could be applied to certain AI systems.[140] The uncertainty surrounding tort law's application to AI makes common law tort an economically inefficient pathway to reasonable and uniform standards and creates disincentives for companies utilizing and investing in the development of AI systems.[141]

B. AI Development in the United States

While the United States has been unable to implement comprehensive legislation, Congress has, at the same time, pushed for the advancement of AI systems through research initiatives.[142] The Select Committee on Artificial Intelligence was established in May 2018 and rechartered on January 5, 2021 "in accordance with the National Artificial Intelligence Act of 2020 … with a broader scope and membership."[143] The Committee is comprised of heads of agencies and advises the White House on inter-agency AI Research and Development priorities.[144] It is an attempt to "provide[] a formal mechanism for inter-agency policy coordination and the development of federal AI activities; and addresses national and international AI policy matters."[145] The National Science Foundation has also established a research initiative for AI technology that invested $220 million in institutes in forty states and the District of

---

139 *Id.*

140 *Id.* at 201–02.

141 *Id.* at 199, 201–02.

142 HARRIS, *supra* note 4, at 18–27; *see* Press Release, U.S. Department of Commerce, Department of Commerce Establishes National Artificial Intelligence Advisory Committee (Sept. 8, 2021), https://www.commerce.gov/news/press-releases/2021/09/department-commerce-establishes-national-artificial-intelligence ("The committee is to provide recommendations on topics including the current state of U.S. AI competitiveness; progress in implementing the Initiative; the state of science around AI; issues related to AI workforce, including barriers to employment supporting opportunities for historically underrepresented populations; how to leverage initiative resources; the need to update the initiative; the balance of activities and funding across the initiative; the adequacy of the National AI R&D Strategic Plan; management, coordination, and activities of the initiative; adequacy of addressing societal issues; opportunities for international cooperation; issues related to accountability and legal rights; and how AI can enhance opportunities for diverse geographic regions.")

143 *Id.* at 17–18; SCAI – Select Committee on Artificial Intelligence, https://www.ai.gov/about/#SCAI-SELECT-COMMITTEE-ON-AI (last visited Oct. 23, 2021).

144 HARRIS, *supra* note 4, at 17–18.

145 *Id.* at 17.

Columbia.[146] The United States has also devoted defense funds to develop AI systems within a military context.[147]

Despite these steps in the right direction, the United States is lagging severely behind in government-funded AI research.[148] In comparison, the European Commission had funded close to €20 billion for AI development by 2020 and has promised billions more for AI research through 2027.[149] The Chinese government has invested even more, with at least one estimate of $70 billion committed in 2020.[150] The majority of funding for AI development in the United States has come from the private sector.[151] The dominance of private sector AI development in the United States is diminishing.[152] While Chinese interests previously invested directly in U.S. tech companies, government funding in China has shifted those investments to remain at home.[153] In 2018, forty-eight percent of all worldwide venture capital funds went to firms in China, and Chinese AI startups received more funding than their U.S. counterparts by around $500 million.[154] The United States has no concrete plan for AI investment, and the reliance on private funds will not suffice to keep pace with research investments in China and even the EU.[155]

Although the U.S. government has identified some of the potential issues with unregulated AI, it is not moving with the sense of urgency that the increasing presence of AI in the industry likely requires.[156] Even within the U.S.

---

146 Houser & Raymond, *supra* note 17, at 154; *see also Artificial Intelligence at NSF*, NAT'L SCI. FOUND. (updated July 30, 2021), https://www.nsf.gov/cise/ai.jsp.

147 *Id*. at 155 (citing Drew Harwell, *Defense Department Pledges Billions Toward Artificial Intelligence Research*, WASH. POST (Sept. 7, 2018, 7:39 AM), https://www.washingtonpost.com/technology/2018/09/07/defense-department-pledges-billions-toward-artificialintelligence-research/).

148 *Id*. at 154–55.

149 *Id*. at 148–49 (citing *AI in Europe: Funding Hits [euros] 20 Billion*, NEXT GENERATION INTERNET (Jan. 8, 2019), https://www.ngi.eu/news/2019/01/08/ai-in-europe-funding-hits-e20-billion/).

150 *Id*. (citing Oriana Pawlyk, *China Leaving U.S. Behind on Artificial Intelligence: Air Force General*, MILITARY.COM: DEFENSE TECH (July 30, 2018), https://www.military.com/defensetech/2018/07/30/china-leaving-us-behind-artificial-intelligence-air-force-general.html).

151 *Id*. at 153–54.

152 *Id*. at 156.

153 *See* Houser & Raymond, *supra* note 17, at 156.

154 *Id*.

155 *See generally id*.

156 *Id.* at 39–43; *see* Up Market Research, *Global Artificial Intelligence Market Is Expected To Set A New Benchmark With A CAGR Of 40.2% By 2028*, PRNEWSWIRE (Oct. 19, 2021, 10:08 AM), https://www.prnewswire.com/news-releases/global-artificial-intelligence-market-is-expected-to-set-a-new-benchmark-with-a-cagr-of-40-2-by-2028—up-market-research-301403520.html (reporting that the global AI market is "expected to grow at a compound annual rate (CAGR) of 40.2% between 2021 and 2028"); CATHY

government, agencies are beginning to use algorithms to determine the distribution of public benefits to the detriment of many Americans.[157] The United States has recognized that the advancement of AI technology, as it relates to geopolitical power, is vital to maintaining global influence, and it works in tandem with data collection practices.[158] Government leadership is, therefore, reluctant to stymie AI development through either AI regulation or, alternatively, through data privacy regulation.[159] Accordingly, the looming

O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (1st ed. 2016) (explaining how AI is causing and, if unregulated, will cause extreme negative societal effects related to college admissions, advertising, the judicial system, employment, credit, insurance, and social standing); *see also* Heidi Leford, *Millions of Black People Affected by Racial Bias in Health-Care Algorithms*, NATURE NEWS (Oct. 26, 2019) ("An algorithm widely used in U.S. hospitals . . . was less likely to refer black people than white people who were equally sick to programmes that aim to improve care for patients with complex medical needs. Hospitals and insurers use the algorithm and others like it to help manage care for about 200 million people in the United States each year."); Jeff Larson, Surya Mattu, Lauren Kirchner & Julia Angwin, *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm (finding that an AI tool meant to predict recidivism of former criminals incorrectly judged black defendants as higher risk for recidivism far more often than it did so for white defendants, while also incorrectly flagging white defendants as low risk more often than black defendants); Heather J. Meeker & Amit Itai, *Bias in Artificial Intelligence: Is Your Bot Bigoted?*, BL: TECH. & TELECOM L. (Oct. 19, 2020), https://news.bloomberglaw.com/tech-and-telecom-law/bias-in-artificial-intelligence-is-your-bot-bigoted ("We are just starting to understand how much of our human biases make their way into AI. For example, the data that we use to train AI may be selected in a biased way. But even if companies building AI systems do not intend to discriminate, the tools they use can still have discriminatory outcomes. And because software controls so much of our day-to-day lives, the result is systemic bias that can be challenging to eradicate."); Press Release, Dep't of Just., Justice Department and EEOC Warn Against Disability Discrimination (May 12, 2022), https://www.justice.gov/opa/pr/justice-department-and-eeoc-warn-against-disability-discrimination (stating that employers using AI could be discriminating against applicants with disabilities).

[157] *See* Michele E. Gilman, *Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice*, 52 ARIZ. ST. L.J. 368, 371–72 (2020) ("Government agencies are turning to algorithms to apportion public benefits, yet these automated decision-making systems lack transparency, leaving thousands of people adrift without state support and not knowing why.").

[158] *See* Dina Temple-Raston, *China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying*, NPR: INVESTIGATIONS (Aug. 26, 2021), https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying ("Officials believe that the [Microsoft Exchange data] breach was in the service of something bigger: China's artificial intelligence ambitions."); Cameron F. Kerry, *Protecting Privacy in an AI-Driven World*, BROOKINGS (Feb. 10, 2020), https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/ ("As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed."); Eva Xiao, *China Passes One of the World's Strictest Data-Privacy Laws*, WALL ST. J. (Aug. 20, 2021), https://www.wsj.com/articles/china-passes-one-of-the-worlds-strictest-data-privacy-laws-11629429138 ("The national privacy law, China's first, closely resembles the world's most robust framework for online privacy protections, Europe's General Data Protection Regulation, and contains provisions that require any organization or individual handling Chinese citizens' personal data to minimize data collection and to obtain prior consent.").

[159] *China Has Won AI Battle with the U.S., Pentagon's Ex-software Chief Says*, REUTERS (Oct. 11, 2021), https://www.reuters.com/technology/united-states-has-lost-ai-battle-china-pentagons-ex-software-chief-says-

presence of China's AI prowess has been the only apparent motivation for the U.S. government's direct investment in research initiatives and training.[160] China is often mentioned as the main driving force for U.S. AI development in published media and oversight reports.[161] However, as mentioned above, the focal point of research funding has been for the military and defense sector.[162] Especially in relation to AI identification tools and biometric information processing, this emphasis on national defense by the U.S. government may prevent the United States from adopting similar regulations to those that are included in the AIA despite public concern about AI in law enforcement.[163]

2021-10-11/; Ross Andersen, *The Panopticon is Already Here*, THE ATLANTIC (Sept. 2020), https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

[160] The CRS report explains that the government fears economic loss and the disregard for democratic norms and values. HARRIS, *supra* note 4, at 38; s*ee* Andersen, *supra* note 159 ("The emergence of an AI-powered authoritarian bloc led by China could warp the geopolitics of this century. It could prevent billions of people, across large swaths of the globe, from ever securing any measure of political freedom.").

[161] HARRIS *supra* note 4, at 7–8, 25, 26, 38, (citing Stanford AI Index Report, *supra* note 73; U.S. Congress, Joint U.S.-China Economic and Security Review Commission, Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy, 116th Cong., 1st sess., June 7, 2019; U.S.-China Economic and Security Review Commission, 2020 Annual Report to Congress, December 2020, p. 107, at https://www.uscc.gov/files/001592); *see also* David Ignatius, *China's Application of AI Should Be a Sputnik Moment for the U.S. but Will It Be?*, WASH. POST (Nov. 6, 2018), https://www.washingtonpost.com/opinions/chinas-application-of-ai-should-be-a-sputnik-moment-for-the-us-but-will-it-be/2018/11/06/69132de4-e204-11e8-b759-3d88a5ce9e19_story.html ("'China is the OPEC of data,' argues Webb. In a totalitarian society, every human and social interaction feeds a vast pool of structured data for machines to ingest. The Chinese government can then commandeer companies and people, as needed. America may need an 'AI czar,' argues Ashton B. Carter, former secretary of defense for President Barack Obama. That's because no current agency or White House office is empowered to coordinate an effort as complicated as the Manhattan Project, which built a nuclear weapon, or the 'space race' that put a man on the moon."); *but see* Tim Culpan, *China Isn't the AI Juggernaut the West Fears*, BLOOMBERG: TECH. & IDEAS (Oct. 11, 2021, 6:00 PM) (explaining that Chinese AI expertise only excels in computer vision related to its surveillance state, while the U.S. is the leader in machine learning and network technologies that have much broader applications); John Naughton, *Fear Itself is the Real Threat to Democracy, Not Tall Tales of Chinese AI*, THE GUARDIAN (Mar. 6, 2021) (comparing fear of Chinese AI to fear of communism in the Cold War era, but highlighting the fact that this AI race will force U.S. companies to provide the government with all of their personal data on American citizens).

[162] *See* Houser & Raymond, *supra* note 17, at 147, 151.

[163] *See* Letter from Senator Ron Wyden et al. to Gene L. Dorado, Comptroller General of the United States (July 31, 2018), https://www.wyden.senate.gov/imo/media/doc/073118%20GAO%20Facial%20Recognition%20Request%20(as%20submitted).pdf ("We write to you today to request that [Government Accountability Office] examine and evaluate commercial and law enforcement use of facial recognition technologies. These technologies raise serious concerns about individual privacy rights and the disparate treatment of minority and immigrant communities within the United States."); Hill, *supra* note 52; Rashida Richardson, Jason Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. 192 (2019) ("[N]umerous jurisdictions suffer under ongoing and pervasive police practices replete with unlawful, unethical, and biased conduct. This conduct does not just influence the data used to build and maintain predictive systems; it supports a wider culture of suspect police practices and ongoing data manipulation. Add to this the lack of oversight and accountability measures regarding

However, even large U.S. tech companies such as Google and Microsoft are eager for a comprehensive regulatory framework and have released their own best practices for AI implementation.[164] The willingness of tech companies to accept regulation lends credence to the thought that AI regulation could improve AI development rather than hinder it.[165] Public trust in AI will create a larger market for those technologies, and there is currently a strong distrust among the public of unregulated AI systems.[166]

III. LESSONS LEARNED FROM DATA PRIVACY AND THE GDPR

AI and data are inseparable concepts. AI requires data with which to train, and any regulation that affects data will consequently regulate AI. Data privacy regulations have already developed in the EU and the United States due to public concern with personal data security. This section will explore existing data privacy regulations in the EU and the United States and explain how those regulations can provide a foundation for AI regulatory schemes.

police data collection, analysis, and use, and it becomes clear that any predictive policing system trained on or actively using data from jurisdictions with proven problematic conduct cannot be relied on to produce valid results without extensive independent auditing or other accountability measures."); *c.f.* DEP'T OF HOMELAND SEC., S&T ARTIFICIAL INTELLIGENCE & MACHINE LEARNING STRATEGIC PLAN (Aug. 2021), https://www.dhs.gov/sites/default/files/publications/21_0730_st_ai_ml_strategic_plan_2021.pdf (summary of DHS plan for developing AI); U.S. CUSTOMS AND BORDER PROTECTIONS, *Biometrics* https://biometrics.cbp.gov/ (showcasing new biometrics facial recognition use by customs); *but see* Kristin Finklea et al., Cong. Rsch. Serv., R46586, Federal Law Enforcement Use of Facial Recognition Technology 12–15 (Oct. 27, 2020) (stating that "56% of surveyed Americans indicated that they trust law enforcement agencies to use FRT responsibly, and 59% indicated it is acceptable for law enforcement agencies to use these technologies to assess security threats in public." (citing Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, PEW RSCH. CTR. (Sept. 5, 2019))).

164 *Responsible AI practices*, GOOGLE, https://ai.google/responsibilities/responsible-ai-practices/ (last visited Sept. 20, 2021); *Responsible AI*, MICROSOFT, https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6 (last visited Oct. 17, 2021).

165 *See* Mark MacCarthy, *AI Needs More Regulation, Not Less*, BROOKINGS (Mar. 9, 2020) ("Smart regulation . . . that gets out in front of emerging technology can protect consumers *and* drive innovation. In the last several decades, however, policymakers have forgotten this beneficial side effect of regulation, preferring to give industry players free rein to deploy emerging technologies as they see fit.").

166 *See Artificial Intelligence Act*, *supra* note 25, at 3; Kate Schmidt & Matt Furlow, *Investing in Trustworthy AI*, DELOITTE: AI INST. AND CHAMBER TECH. ENGAGEMENT CTR. 38 (2021), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-investing-in-trustworthy-ai-full-report-new.pdf ("If the risks posed by unmanaged development of AI are left unaddressed, reductions in consumer and worker trust may inhibit the long-term growth and adoption of AI technologies, and discourage the private sector from investing in AI-enabled solutions and limit the benefits of AI and on overall economic growth.").

A. Data Privacy in the European Union

Regardless of its successes and failures, the GDPR provides a strong working model for regulatory action related to data protection and AI.[167] The United States should recognize the goals of the GDPR and the AIA and adopt a similarly comprehensive approach to protect its own citizens from the dangers of these increasingly ubiquitous digital tools and to reap the benefits of harmonizing its regulations with those of the EU.[168]

The adoption of the GDPR exemplifies the importance the EU has placed on data protection and fair AI.[169] Under the Charter of Fundamental Rights of the European Union (Charter), protection of private communications (Article 7) and personal data (Article 8) are considered fundamental rights.[170] The Charter further provides that restrictions on those rights must be proportional to the "objectives of general interest."[171] With the GDPR in 2018, the EU demonstrated its commitment to these fundamental rights and its recognition of the dangers that data protection faced without a comprehensive regulatory scheme.[172] The GDPR imposes many requirements on companies that use data, such as ensuring data security through methods like encryption or pseudonymization and providing an easy method for individuals to request that

---

[167] *See* Estelle Massé, *Three Years Under the EU GDPR: An Implementation Progress Report*, ACCESSNOW (May 2021) (explaining that despite the GDPR's incredible importance for data protection, there has been systematic failures in enforcement that are jeopardizing the success of the regulations).

[168] *See* Ursula Morgenstern, *Ethics by Design: Steps to Prepare for AI Rules Changes*, FORBES (Oct. 21, 2021), https://www.forbes.com/sites/cognizant/2021/10/21/ethics-by-design-steps-to-prepare-for-ai-rules-changes/?sh=17a720a14b2f (the GDPR in tandem with the Artificial Intelligence Act will create a system of "[e]thics by design").

[169] *See* WHAT IS GDPR, THE EU'S NEW DATA PROTECTION LAW?, https://gdpr.eu/what-is-gdpr/ (last visited Oct. 24, 2021) ("The right to privacy is part of the 1950 European Convention on Human Rights, which states, 'Everyone has the right to respect for his private and family life, his home and his correspondence.' From this basis, the European Union has sought to ensure the protection of this right through legislation. As technology progressed and the Internet was invented, the EU recognized the need for modern protections."); Todd Ehret, *Data Privacy and GDPR at One Year, a U.S. Perspective: Part One - Report Card*, REUTERS: FIN. REG. F. (May 22, 2019), https://www.reuters.com/article/bc-finreg-gdpr-one-year-report-card-part-idUSKCN1SS2K5 ("The regulation was created with a deliberate global reach and set a new level of obligations and expectations regarding data protection, security, and management.").

[170] Charter of Fundamental Rights of the European Union arts. 7–8, Oct. 26, 2012, 2012 O.J. (C 326) 397–98.

[171] *Id.* art. 52.

[172] *See* WHAT IS GDPR, *supra* note 169; *see also* GDPR, *supra* note 31, at 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right.").

a company deletes all of their data.[173] Furthermore, the GDPR imposes regulations on companies that transfer personal data of E.U. citizens to foreign countries under Chapter V.[174] Those restrictions include the requirement that the company guarantees adequate protection of data in the foreign country.[175]

The GDPR often effectively regulates companies extraterritorially because many major data collectors are U.S. companies. The provisions in Chapter V have resulted in numerous fines on U.S. companies that were unable to adapt to the regulations.[176] Article 83 states that companies that infringe the provisions in Chapter V are subject to administrative fines of up to the greater value between €20 million and four percent of "total worldwide annual turnover of the preceding financial year."[177] The GDPR creates a private right of action through which complaints are lodged to the supervisors established by the GDPR in each Member State and litigated in national courts.[178] Google was fined €50 million

---

[173] *See* GDPR CHECKLIST FOR DATA CONTROLLERS, https://gdpr.eu/checklist/ (last visited Oct. 24, 2021) (checklist for compliance); GDPR, *supra* note 31, arts. 17, 32 (detailing the 'right to be forgotten' and security requirements).

[174] GDPR, *supra* note 31, arts. 44–50; *see* Ben Wolford, GDPR COMPLIANCE CHECKLIST FOR U.S. COMPANIES, https://gdpr.eu/compliance-checklist-us-companies/ (last visited Oct. 24, 2021); Ehret, *supra* note 169 ("GDPR is designed to protect the privacy rights of EU individuals but applies to all companies processing or controlling the personal information of EU residents, regardless of where those firms are located.").

[175] GDPR, *supra* note 31, arts. 45–46 (the European Commission can determine in advance whether a particular country outside of the EU provides "an adequate level of protection" and therefore can receive data; if the commission decides that country does not provide adequate protection, a company must guarantee adequate safeguards to its data); *see Adequacy Decisions*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Oct. 24, 2021) ("The European Commission has so far [recognized] Andorra, Argentina, Canada (commercial [organizations]), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.").

[176] U.S. INT'L TRADE COMM., ONE YEAR IN: GDPR FINES AND INVESTIGATIONS AGAINST U.S.-BASED FIRMS (Sept. 2019), https://www.usitc.gov/publications/332/executive_briefings/gdpr_enforcement.pdf ("Since May 2018, EU member state data regulators have imposed fines on many companies for GDPR violations. Although a majority of these fines have been low in value, the EU has collectively imposed more than €380 million ($417 million) in total fines under GDPR. The second and third largest fines were imposed on U.S.-based multinational companies Google and Marriott [], while the largest so far was a £183 million ($229 million) fine imposed by the UK Information Commission Office (UK ICO) against British Airways."); *see also Three Years of GDPR: the Biggest Fines so Far*, BBC: TECH (May 24, 2021), https://www.bbc.com/news/technology-57011639; Natasha Lomas, *WhatsApp Faces $267M Fine for Breaching Europe's GDPR*, TECHCRUNCH (Sept. 2, 2021); Stephanie Bodoni, *Amazon Gets Record $888 Million EU Fine Over Data Violations*, BLOOMBERG: TECH (July 30, 2021, 7:43 AM).

[177] *Compare* GDPR, *supra* note 31, art. 83 *with Artificial Intelligence Act*, *supra* note 25, at 82–83.

[178] *See* Ehret, *supra* note 169 (stating that "under the GDPR, individuals are able to file claims for 'material or non-material damage' as a result of a breach of the GDPR [and] not-for-profit organizations have the right to lodge a complaint on behalf of an individual"); Todd Ehret, *Data privacy and GDPR at One Year, a U.S. Perspective: Part Two - U.S. Challenges Ahead*, REUTERS: FIN. REG. F. (May 29, 2019),

in January of 2019 by the French supervising authority for deficient transparency, data reporting, and consent issues relating to personalization the of advertisements.[179] However, this fine only accounted for 0.04% of Google's global revenue, and other fines issued by the European national data protection authorities, or DPAs, have been much less.[180]

B. Data Privacy in the United States

Just as with AI, the United States does not have any comprehensive federal regulations pertaining to data protection currently.[181] There are limited restrictions related to data in certain industries such as Health Insurance Portability and Accountability Act (HIPAA); Fair Credit Reporting Act (FCRA); Family Educational Rights and Privacy Act (FERPA); The Gramm-Leach-Bliley Act (GLBA); Electronic Communications Privacy Act (ECPA); Children's Online Privacy Protection Act (COPPA); and Video Privacy Protection Act (VPPA) that relate to health data, credit reporting, education records, loan or investment data, wiretaps, children, and Video Home System (VHS) rental records.[182] The FTC Act also allows the FTC to pursue actions against companies that deceive users into unknowingly parting with personal data.[183] Three states have passed data privacy laws; however, California's

https://www.reuters.com/article/us-bc-finreg-gdpr-report-card-2/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-two-u-s-challenges-ahead-idUSKCN1SZ1US ("A new risk emerging from GDPR is the risk of private litigation. Under GDPR, individuals are able to claim for 'material or non-material damage' as a result of a breach of the GDPR.").

179 Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

180 *See* Ehret, *supra* note 169; *see also* Massé, *supra* note 167, at 9–12 (explaining how DPAs are having difficulty enforcing GDPR regulations in smaller countries, like Ireland and Luxembourg, because of the disparity between the DPAs' budgets and the companies' revenue).

181 *See* Klosowski, *supra* note 30 ("The data collected by the vast majority of products people use every day isn't regulated. Since there are no federal privacy laws regulating many companies, they're pretty much free to do what they want with the data, unless a state has its own data privacy law."). The United States is a signatory to the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which "are intended to be used as a basis for new, or to be built into existing, data protection legislation." However, the Guidelines are non-binding, and the United States has failed to incorporate their provision into domestic law. *See* Monika Kuschewsky, *What Does the Revision of the OECD Privacy Guidelines Mean for Businesses?*, LEX AB EXTRA (Oct. 22, 2013), https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf.

182 Klosowski, *supra* note 30.

183 *See id.* ("The FTC can also investigate violations of marketing language related to privacy, as it did when it issued a complaint against Zoom for deceiving users by saying video chats were end-to-end encrypted." (citing Press Release, Fed. Trade Comm'n, FTC Requires Zoom to Enhance its Security Practices as Part of

Consumer Privacy Act (CCPA) is the only law in the United States that creates a private right of action.[184] Despite the growing number of states introducing litigation,[185] the federal government has yet to introduce an act to ensure uniformity around data protection.[186] While not unimportant, the only comprehensive schemes of note in the United States are national security laws, such as the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, which allow the U.S. Intelligence Community to use personal data for surveillance of foreign citizens or of U.S. citizens on U.S. soil only after a court order.[187] Presidential Policy Directive 28 also allows for the collection of bulk data, irrespective of origin, but restricts access to situations where there are terrorist, espionage, or military threats.[188]

C. Attempts to Synchronize Data Policies Across the Atlantic

To satisfy U.S. commercial desire for European data, the EU and the United States have attempted to create privacy frameworks to facilitate the transfer of personal data within the guidelines of the GDPR.[189] The first attempt was the U.S.-EU Safe Harbor Framework, but that was invalidated by the Court of Justice of the European Union (CJEU), which is the appellate authority under

---

Settlement (Nov. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement)).

184 Ehret (Part Two), *supra* note 178; *see* Sarah Rippy, U.S. *State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (last updated Sept. 16, 2021) (includes a pdf chart that shows progress of current legislation, the consumer rights they protect, and the obligations they impose on businesses).

185 *See* Rippy, *supra* note 184 (showing nine total bills or statutes, four that include a private right of action, currently in state legislatures which are being considered in Massachusetts, Minnesota, New York, North Carolina, Ohio, and Pennsylvania).

186 *See* Klosowski, *supra* note 30 (identifying that data-breach law differs from region to region and currently there are "at least 54 different laws" related to data breach notifications).

187 50 U.S.C. §§1801-1885(c); Exec. Order No. 12,333, 46 Fed. Reg. 599941 (Dec. 4, 1981); *see also* DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., 21-129, AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EXECUTION OF ITS WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS (Sept. 2021), https://oig.justice.gov/sites/default/files/reports/21-129.pdf ("The FBI's Woods Procedures are designed to ensure FISA applications are 'scrupulously accurate' and require agents to document support for all factual assertions contained in them. However, our audit found numerous instances where this did not occur.").

188 *See* Press Release, Off. of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (issuing guiding principles on intelligence gathering and data collection).

189 Chris D. Linebaugh & Edward C. Liu, CONG. RES. SERV., R46724, EU DATA TRANSFER REQUIREMENTS AND U.S. INTELLIGENCE LAWS: UNDERSTANDING SCHREMS II AND ITS IMPACT ON THE EU-U.S. PRIVACY SHIELD 1 (Mar. 17, 2021), https://crsreports.congress.gov/product/pdf/R/R46724 ("[T]he EU-U.S. Privacy Shield (Privacy Shield) [was] developed by the European Union (EU) and the United States to facilitate cross-border transfers of personal data for commercial purposes.").

Article 267 of the Treaty on the Functioning of the European Union (TFEU) and can rule on preliminary questions at the request of national courts by the same article in the TFEU.[190] The second iteration was the Privacy Shield Framework, developed in 2016.[191] However, this was also invalidated in the 2020 CJEU case *Data Protection Commissioner v. Facebook Ireland, Ltd. and Maximillian Schrems*, also referred to as *Schrems II*.[192] Maximillian Schrems, a famous privacy rights advocate and law graduate from the University of Vienna, has made it a personal mission to prevent Facebook from providing the U.S. government with information about EU citizens in the wake of Edward Snowden's disclosures regarding the PRISM surveillance program, which was instituted under FISA.[193] In *Schrems II*, the CJEU decided that the Privacy Shield framework did not comport with the GDPR due to "(1) the lack of ex-ante limitations ensuring that surveillance programs abide by the 'principle of proportionality' (i.e., that the programs only collect data that is strictly necessary); and (2) the ineffective ex-post redress for individuals" under FISA and Executive Order 12333.[194]

The CJEU did hold that Standard Contractual Clauses (SCCs) can be used as an alternative to the Privacy Shield framework, but the data "exporters" must ensure that the third-party country receiving the data is compliant with the GDPR.[195] While the CJEU did not directly rule on whether the U.S. offers adequate protection for SCCs, this case highlights that there is undoubtedly a

---

[190] *Id.* at 3.

[191] *Id.* at 3–4.

[192] *Id.* at 5–6; *see* Recent Case, *Data Protection Commissioner v. Facebook Ireland Ltd. Court of Justice of the European Union Invalidates the EU-U.S. Privacy Shield*, 134 Harv. L. Rev. 1567 (2021) ("[T]he CJEU found that U.S. limitations on data protection violate the principle of proportionality. In order to satisfy the requirement of proportionality, legislation must incorporate 'clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.' Moreover, any legislation infringing upon an EU data subject's data privacy rights must be 'limited to what is strictly necessary.'").

[193] Hannah Kuchler, *Max Schrems: The Man Who Took on Facebook – and Won*, FIN. TIMES (Apr. 5, 2018), https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544 ("Schrems' journey started when, as a 23-year-old law student, he requested his personal data from Facebook for a college paper. He was shocked to find the social network had amassed 1,200 pages — everything he'd ever 'Liked' and every private message he'd ever sent. He filed 22 complaints claiming that Facebook was breaking European data protection law, undermining the fundamental right to privacy. Back in 2011, Schrems was already arguing that Facebook was a 'monopoly' that needed special attention from regulators.").

[194] Linebaugh & Liu, *supra* note 189, at 5–6.

[195] *Id.* at 3, 6–8 ("While *Schrems II* invalidated Privacy Shield, it still left room for data transfers to the United States based on SCCs or other mechanisms under Article 46 of the GDPR. Even when relying on these mechanisms, the CJEU explained that data exporters must still analyze the law of the non-EU country and adopt any 'supplementary measures' necessary to ensure the adequate protection required under EU law.").

divide between the U.S. and EU policy regarding personal data protection.[196] This problem of data transfer may be resolved soon by the current executive administration; the United States and the EU have agreed in principle to a replacement for the Privacy Shield entitled the Trans-Atlantic Data Privacy Framework, which will create a mechanism through which EU citizens can request redress from the United States for unwanted data collection within its borders.[197] Despite this step towards cooperation, the additional compliance measures potentially imposed on U.S. companies by the AIA will further exemplify and exacerbate the split between U.S. and E.U. policy on AI and may weaken diplomatic relations.[198] If the divergence of policy between the U.S. and the E.U. continues, the costs of ensuring transatlantic compliance could create a greater boundary to developing AI systems which would have anticompetitive and anti-innovation implications.[199]

D. Data Regulation is a Supplement, not a Substitute, to AI Regulation

Although, in effect, the GDPR already governs the use of AI that requires personal data, if the AIA is adopted, there will be further consequences for

---

[196] *Id.* at 13 ("While not directly addressing the issues raised in *Schrems II*, some commentators have also maintained that the United States' adoption of a comprehensive federal data protection law applicable to commercial entities could facilitate transatlantic data transfers.").

[197] Press Release, The White House FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/. Notably, this new agreement does not offer redressability for citizens of the United States regarding the collection of their personal data. *See id.*

[198] ULRIKE FRANKE, ARTIFICIAL DIVIDE: HOW EUROPE AND AMERICA COULD CLASH OVER AI, EUR. COUNCIL ON FOREIGN RELS. 9–10 (Jan. 20, 2021), https://ecfr.eu/wp-content/uploads/Artificial-divide-How-Europe-and-America-could-clash-over-AI.pdf ("[M]any Europeans have expressed scepticism about the extent to which Europe and the US are indeed aligned on ethical AI principles. For example, the Danish national AI strategy argues for a common ethical and human-centred basis for AI. It describes ethical AI as a particularly European approach: 'Europe and Denmark should not copy the US or China. Both countries are investing heavily in artificial intelligence, but with little regard for responsibility, ethical principles and privacy.' Many Europeans feel that the US 'has no idea how to regulate' cyberspace and continues to show little enthusiasm for doing so. The EU, however, likes to think of itself as a trailblazer when it comes to digital rights, such as the 2014 'right to be forgotten' or the 2018 General Data Protection Regulation.").

[199] *See* Lydia Bayley, *The Patchwork Paradox: Data Privacy Regulation and the Complications of Compliance*, LOYOLA UNIV. OF CHI.: INSIDE COMPLIANCE (Sept. 1, 2020), http://blogs.luc.edu/compliance/?p=3142 ("All of these variations on data privacy across the United States leave many experts questioning how businesses can possibly ensure adherence to all of these laws without incurring massive compliance costs[, but] … the majority of breach-notification statutes are, in fact, rather similar."); Bessen et al., *supra* note 68, at 18.

companies developing AI systems.[200] The new requirements of the AIA highlight the difference in regulating the data used to train AI systems and the AI systems themselves.[201] AI requires data to function properly, but AI exists without data and can manipulate data, thereby creating dangers outside of data collection alone.[202] The AIA supplements the GDPR by providing blanket protection over specific applications where AI could have a markedly negative impact.[203] The regulations in the AIA go beyond data regulation and prohibit dangerous uses of AI regardless of the level or source of the data used.[204] AI regulation is necessary to ensure a limitation on potentially dangerous uses of AI; however, a well-built data protection regime can provide fundamental aid in alleviating those dangers.[205] A well-built data regulation system can help safeguard against the effectiveness of malevolent AI systems, thereby regulating them indirectly.[206] Data regulation can also ensure that citizens can limit the collection of their data and receive adequate notice of when and how their data is used, so citizens can choose not to fuel AI systems of which they disapprove.[207]

The GDPR gives the EU tools to combat civil rights and economic justice issues that can result from the inappropriate use of personal data in AI

---

[200] *See* Marijn Storm & Alex van der Wolk, *Privacy and the EU's Regulation on AI: What's New and What's Not?*, THE J. ROBOTICS, A.I. & L. (Apr. 22, 2021), https://www.mofo.com/resources/insights/210422-privacy-eu-regulation-ai.pdf?#zoom=100 ("Compared to the GDPR, the Regulation introduces new obligations for vendors of AI systems, prohibits certain very high-risk AI systems, and introduces more specific requirements for high-risk AI systems and users thereof.").

[201] The GDPR does not limit the way data can be used by AI systems. *Id.* ("Although the GDPR imposes stringent requirements on certain processing activities, it does not outright prohibit any activities.").

[202] *Id*.

[203] *Id*.

[204] *Id*.

[205] *See* William Davidow & Michael S. Malone, *Don't Regulate Artificial Intelligence: Starve It*, SCI. AM, (May 4, 2020), https://blogs.scientificamerican.com/observations/dont-regulate-artificial-intelligence-starve-it/ ("If AI systems and the algorithms in charge of 'virtual prisons' cannot get their hands on this personal information, cannot indulge their insatiable hunger for this data, they necessarily will become much less intrusive and powerful.").

[206] *See* Tjerk Timan et al., *The Role of Data Regulation in Shaping AI: An Overview of Challenges and Recommendations for SMEs*, *in* THE ELEMENTS OF BIG DATA VALUE 355, 373 (2021) ("Looking ahead, cybersecurity will play a key role in the development of AI and as such is a key condition for AI to shape.").

[207] *See id.* at 375; Gilman, *supra* note 157, at 373–374 ("As a piece of legislation, the GDPR does not contain tools to dismantle oppressive structures within the economy and society that technology magnifies, but it does enhance transparency and accountability, which in turn can serve social justice movements. With greater knowledge of and control over personal data flows, Americans can consider other substantive privacy interventions that might be necessary to advance economic justice, such as limitations on targeted advertising, facial recognition technology, workplace surveillance, and the like.").

systems.[208] A similar system in the United States would ensure a more robust protection of the rights of citizens when their data is used in AI.[209] The GDPR includes five specific provisions to aid in protecting citizen's rights in the EU: "(1) the right to an explanation, (2) the right not to be subject to decisions based on automated profiling, (3) the right to be forgotten, (4) a requirement of public participation, and (5) robust implementation and enforcement."[210] The GDPR requires processors of personal data to provide "meaningful information about the logic involved" in algorithmic decision-making, which includes a description of "(1) the categories of data used in processing; (2) the relevance of the data; (3) how profiles are built; (4) the relevance of the profile to the decision-making process; (5) and how the profile is used for an individualized decision."[211] This requirement goes beyond an outcome-based approach to regulation and can help identify potentially harmful algorithms before the effects come to fruition and uncover biases that are not otherwise readily ascertained.[212] The GDPR also prevents certain types of data from being used in automated decision-making all together without explicit consent, including "racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, sex life, sexual orientation, and genetic data."[213] Such bars provide a safeguard against obvious pathways to discriminating algorithms.[214]

Automated decision-making has the potential to negatively affect lower-income individuals to a greater extent than others.[215] Economic advancement is already difficult in the United States: currently, "[f]orty percent of children born in the bottom quintile of the income scale will remain there their entire lives."[216] AI may perpetuate similar economic immobility if institutions incorporate similar statistics to decide when to extend opportunities like loans to individuals.[217] Establishing the legal right to exclude the use of personal data in

---

208 Gilman, *supra* note 157, at 373–74.

209 *Id.* at 374, 399–411.

210 *Id.* at 374, 412–43.

211 *Id.* at 416.

212 *Id.* at 414–16; *but see id.* at 422–24 (explaining that "advertising for payday loans and for-profit educational institutions, which are targeted to minority and low-income people but would rarely appear in the social media feed of a high-income earner" is not encompassed by Article 22 of the GDPR and should be regulated by restricting data processing in a particular business sector, in the same manner as proposed in the AIA).

213 *Id.* at 420–21.

214 *Id.*

215 *Id.* at 424–25.

216 *Id.*

217 *Id.*

decision-making processes can help mitigate the harm of automation for people with low-income backgrounds.[218] The right to be forgotten can also aid those whose past financial problems or criminal records otherwise hinder them from advancing economically.[219]

The GDPR also includes a provision requiring public participation whenever a proposed automated processing of data will "likely [] result in a high risk to the rights and freedoms of natural persons."[220] Inviting the public's opinion on certain data usage is a decidedly democratic approach that the United States should seek to implement.[221] If the United States adopts a similar system, civil and human rights groups would then have the opportunity to raise red flags about potentially harmful automation and prevent AI systems from evading public scrutiny.[222] However, it is crucially important that public participation is meaningful and that it does not act as false public endorsement of an algorithm.[223] Public participation will serve to inform citizens about harmful uses of data.[224] In turn, broadcasting this information will enable more individuals to exercise their right to protect their data and opt out of automated decision systems that are harmful.[225] The CCPA includes a provision that is similar to this requirement in the GDPR.[226] It asks the California Attorney General to collect input from the public to assist in crafting data regulations.[227] A federal data regulation scheme would greatly benefit from a comparable sentiment.[228]

The GDPR is the current paragon of data regulatory schemes, but flaws in its effectiveness have emerged.[229] Yet, many of the problems that have plagued the implementation of the GDPR in the EU would not necessarily manifest in a

---

218 *Id*.
219 *Id*. at 425–27.
220 *Id.* at 431–39.
221 *Id*.
222 *Id*.
223 *Id*. at 438–39.
224 *Id*. at 431–39.
225 *See id*. at 431–39, 442–43.
226 *Id*. at 442–44.
227 *Id*.
228 *Id*.
229 The GDPR includes a one-stop-shop provision that dictates which member country is the primary venue for complaints related to the GDPR. This creates an issue with enforcement in countries where the data protection agency of the country lacks the resources to properly pursue those claims. *See* Massé, *supra* note 167 ("We have found that the majority of DPAs are experiencing significant problems with the application of the so-called one-stop-shop mechanism, a key tool for the enforcement of the GDPR in cross-border cases.").

similar system constructed in the United States.[230] The United States does not have to deal with the bureaucracy inherent in a 27-country political union or the extended length of time it takes for regulatory schemes to be approved.[231] Even as a federalist state, the U.S. Constitution provides several solid grounds to regulate data collection nationally and across all markets. Furthermore, the United States does not lack the resources that many EU Member States do and can thereby establish itself as the global authority on data regulation.[232] Along with AI regulation, the data protection laws in the United States are being formed independently in different states, and a patchwork system is emerging.[233] An inconsistent framework across the United States may cause confusion, hinder the development of AI, create loopholes in the resulting web of enforcement mechanisms, and inspire a race to the bottom in those states that seek to attract capital by resisting AI regulation.[234] A federal regulatory scheme would function

---

[230] The federal government would not have difficulties regulating big tech companies due to insufficient financial resources. However, big tech regulation may be politically divisive. *See* Enrique Dans, *Congress Rolls Out Some Tough Regulatory Proposals For Big Tech*, FORBES (June 12, 2021), https://www.forbes.com/sites/enriquedans/2021/06/12/congress-rolls-out-some-tough-regulatory-proposals-for-big-tech/?sh=7c37cac043c4 ("Regulating big tech is a complex issue, because controlling the abuses committed by these companies often means reducing the features they offer users, which can make new legislation unpopular."); *but see*, Emily A. Vogels, *56% of Americans Support More Regulation of Major Technology Companies*, PEW RSCH. CTR. (July 20, 2021), https://www.pewresearch.org/fact-tank/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/ ("Growing shares of Americans think major technology companies should face more government regulation, and a majority say that these firms have too much economic power and influence . . . .").

[231] Houser & Raymond, *supra* note 17, at 163.

[232] *See* Kate Kaye, *Congress Moves to Give $1B to FTC to Fund New Bureau to Protect Privacy in Tech Platform Era*, DIGIDAY (Sept. 15, 2021), https://digiday.com/marketing/congress-moves-to-give-1b-to-ftc-to-fund-new-bureau-to-protect-privacy-in-tech-platform-era/ ("A proposal passed by a House committee yesterday would allocate $1 billion to the FTC to staff a new bureau addressing unfair or deceptive practices related to privacy, data security, identity theft and other data abuses."); *see also FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions ("Facebook, Inc. will pay a record-breaking $5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy, to settle Federal Trade Commission charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information.").

[233] *See* Klosowski, *supra* note 30.

[234] *See id.*; Jordan Kovnot, Chase Wright, *As States and Nations Continue to Enact Comprehensive Data Privacy Legislation, Pressure Mounts on the U.S. to Pass a Competing Federal Law in 2021, and Businesses Should Prepare for Compliance*, JD SUPRA (Sept. 10, 2021), https://www.jdsupra.com/legalnews/as-states-and-nations-continue-to-enact-3228942/ ("Foremost, federal data privacy legislation would make clear to consumers which baseline rights they are entitled to when it comes to safeguarding their privacy and personal data and ensure there are appropriate enforcement mechanisms in place, rather than requiring consumers to parse through privacy policies and understand the nuances of various state laws (some of which provide relatively weak protections).").

much more effectively than the emerging patchwork system and clarify the legal landscape for emerging AI technology that it intends to commercialize.[235] The United States should recognize the advantages of the simplicity of a centralized regulatory system over the patchwork system of governance that is emerging relating to data protection.[236] It is important that we regulate the consumption and collection of U.S. data to indirectly police the use of potentially harmful AI.[237]

A federal data governance scheme would have additional positive effects for the United States outside of these AI considerations. Proper data privacy laws would promote cooperation between countries and could prevent foreign governments from easily accessing U.S. citizens' data.[238] Data sets are permanent creations.[239] Unregulated collection of data can have potentially catastrophic consequences if that data falls into the hands of foreign enemies.[240] Disaster is much more likely when there is no requirement for data oversight like that which the GDPR imposes.[241] Currently, outside of the FTC's ability to

---

[235] AI Startups have limited resources to deal with regulation. A simple regulatory scheme, rather than a patchwork of state level laws, would help companies to use less resources in order to comply. *See* Bessen et al., *supra* note 68 at 18 ("Though GDPR drives changes that are important to safeguarding personally identifiable information, there are also costs associated with this increased regulation.").

[236] *See* Michael A. Turner, Patrick D. Walker & Kazumi C. Moore, *Data Flows, Technology, & the Need for National Privacy Legislation*, CHAMBER TECH. ENGAGEMENT CTR. 3 (July 11, 2019), https://americaninnovators.com/wp-content/uploads/2019/07/CTEC_DataPrivacyReport_v5-DIGITAL.pdf ("The proliferation of uncoordinated state laws will result in undue business uncertainty—especially within the tech sector—and raise the specter of a patchwork of data privacy laws that unnecessarily impedes data flows, erodes American competitiveness, and harms overall economic performance.").

[237] *See* Kovnot, *supra* note 234.

[238] *See* Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation is Just a Start*, BROOKINGS: TECH STREAM (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ ("federal data protection regime would place the United States on stronger footing to address concerns posed by Chinese companies without opening up Washington to charges of hypocrisy.").

[239] *See* Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 ("You can't make a data set disappear. Once you post it, and people download it, it exists on hard drives all over the world.").

[240] Two companies that have used Microsoft's MS Celeb data set supply the Chinese government with technology used to track Uighurs and other Muslims in China. *See id*.

[241] See *id.*; *see also* Stacy Cowley, *Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement*, N.Y. TIMES (July 22, 2019), https://www.nytimes.com/2019/07/22/business/equifax-settlement.html ("Major data breaches have become an almost routine occurrence. Last year, the Marriott hotel chain disclosed that thieves had stolen personal details on roughly 500 million guests, an attack that has been attributed to a Chinese intelligence-gathering effort. In May, a security journalist revealed that a major title insurance company, First American Financial Corporation, had left nearly 900 million documents related to mortgage deals online and unprotected.").

regulate data practices, the United States has no federal law that requires any minimum supervision of data sets.[242]

IV. EU AND UNITED STATES' CONCERN ABOUT CHINESE DATA DOMINANCE

This section will explore why the power dynamics among the United States, China, and the EU have impeded U.S. data privacy laws and AI regulation.

With the introduction of the AIA, as with the GDPR, the EU has once again placed the value of fundamental rights over concerns of Chinese dominance, which the United States fears is on the horizon.[243] A popular opinion amongst policymakers and tech company giants is that data is the "new oil."[244] This opinion is prevalent in articles and discussions concerning China's massive amount of data collection.[245] The premise is that for an AI system to be as powerful as possible, it needs to have access to the most amount of data possible, and since China is allowing more data to be collected while at the same time restricting its access, it is thereby winning the data arms race.[246] However, this premise is flawed since data is not directly analogous to oil.[247] While data is the

---

[242] As previously mentioned, certain data types such as medical data do have base requirements for privacy. Klosowski, *supra* note 30. The FTC's ability to regulate the data privacy practices of a company overall has been restricted, and the FTC can only act to correct specific instances of unfair practice. *See* LabMD, Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018) ("In sum, assuming *arguendo* that LabMD's negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a), the Commission's cease and desist order is nonetheless unenforceable. It does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished.").

[243] Franke, *supra* note 198, at 10("[A]t the moment, Europeans do not feel the same urgency as the U.S. when it comes to pushing back against China.").

[244] Justin Sherman & Samm Sacks, *The Myth of China's Big A.I. Advantage*, SLATE (June 13, 2019), https://slate.com/technology/2019/06/data-not-new-oil-kai-fu-lee-china-artificial-intelligence.html ("We hear all the time that 'data is the new oil.' It's the hottest new analogy to describe the ways in which data—primarily, access to data for training machine learning and artificial intelligence systems—is an important strategic resource of the 21st century.").

[245] *See id.* ("The use of the analogy also extends into the so-called A.I. race between the United States and China. According to Kai-Fu Lee, CEO of Sinovation Ventures and author of the book AI Superpowers, 'If data is the new oil, China is the new OPEC.'").

[246] *See id.* ("Because of China's large population and lax rules about government surveillance, the narrative goes, the country as a whole has a strategic A.I. advantage over the United States. In large part, this has been fueled by Kai-Fu Lee's AI Superpowers, in which he argues that access to data for training machine learning systems is the biggest deciding factor in global A.I. dominance."); Natasha Lomas, *Zuckerberg Urges Privacy Carve Outs to Compete with China*, TECHCRUNCH (Apr. 10, 2018), https://techcrunch.com/2018/04/10/zuckerberg-urges-privacy-carve-outs-to-compete-with-china/ (explaining Facebook's desire for U.S. regulators to implement a more lax privacy scheme than the GDPR).

[247] *See* Graham Webster & Scarlet Kim, *The Data Arms Race Is No Excuse for Abandoning Privacy*, FOREIGN POLICY (Aug. 18, 2018), https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-

fuel that AI runs on, it is not an exclusive resource.[248] Most importantly, data may not be the single most important factor in developing AI; generally, there are diminishing returns in the effectiveness of AI systems as more data is used, and "noisy" or low-quality data is typically useless.[249] Abandoning privacy laws has other implications that far outweigh this vague consensus on the true value of data in AI systems.[250]

New Chinese data protection laws offer evidence against pushing for the deregulation of data.[251] China has recently enacted the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) in direct response to the GDPR and U.S. regulations.[252] While PIPL may still leave ample room for surveillance by the Chinese government, China demonstrably does not believe that forgoing increased regulation is necessary to win a so-called arms race related to AI systems.[253]

---

abandoning-privacy/ ("But large data sets are not a cure-all for AI developers. Research indicates that some applications experience rapidly diminishing returns in efficiency as large datasets become larger, and noisy or badly labeled data are of limited utility. Nor will data alone, without theoretical innovations and advanced hardware, drive breakthroughs."); *see also* Chen Sun, Abhinav Shrivastava, Saurabh Singh1, & Abhinav Gupta, *Revisiting Unreasonable Effectiveness of Data in Deep Learning Era*, GOOGLE RESEARCH, CARNEGIE MELLON UNIVERSITY (revised Aug. 4, 2017), https://arxiv.org/pdf/1707.02968.pdf ("Most interestingly, we can see that the performance grows logarithmically as pretraining data expands . . .").

248 Webster, *supra* note 247.

249 *See* Sherman, *supra* note 244 ("There are other key drivers of A.I. development and implementation, such as the hardware on which machine learning algorithms are developed."); Webster, *supra* note 247.

250 *See* Webster & Kim, *supra* note 247 ("Users are the biggest potential losers in this race, with their rights to privacy and personal data protection held up as a challenge to innovation.").

251 *See* Eva Xiao, *China Passes One of the World's Strictest Data-Privacy Laws*, WALL ST. J. (Aug. 20, 2021), https://www.wsj.com/articles/china-passes-one-of-the-worlds-strictest-data-privacy-laws-11629429138 ("China's new privacy framework comes as frustration grows within the government and in Chinese society over online fraud, data theft and data collection by domestic technology giants. For years, loose rules on accessing data allowed domestic companies to quickly develop and adopt new products and technology, but also fueled a black market for consumer data.").

252 *See* Ryan D. Junck et al. , *China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (Nov. 3, 2021), https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws.

253 *See* Xiao, *supra* note 251 (explaining that although the new privacy laws will increase costs for tech companies, they will also "provide new opportunities for third parties who help companies with data management," and address public concerns about facial recognition and algorithmic discrimination); *see also* Press Release, U.S. Department of the Treasury, Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex (Dec. 16, 2021), https://home.treasury.gov/news/press-releases/jy0538 ("The entities identified today are Cloudwalk Technology Co., Ltd.; Dawning Information Industry Co., Ltd.; Leon Technology Company Limited; Megvii Technology Limited; Netposa Technologies Limited; SZ DJI Technology Co., Ltd.; Xiamen Meiya Pico Information Co., Ltd.; and Yitu Limited.").

The PIPL, and to a greater extent, the DSL, highlights how the issue of digital sovereignty plays an important role in AI competition.[254] Digital sovereignty is the idea that data that comes from a particular country belongs to that country.[255] The United States and the EU have not fully embraced the idea of digital sovereignty to the extent that India and China have.[256] AI produces the most accurate results when it is trained with a data set that is comparable to the population in which it is implemented.[257] Therefore, regulation of data prevents foreign AI developers from entering a particular market by limiting their effectiveness.[258] Without free access to a country's data, foreign competitors are required to go through additional steps to enter that other country's market.[259] If the United States wants to limit the impact of Chinese AI development within its borders, it can do so through data privacy laws.[260] Furthermore, other

[254] *See* Junck et al., *supra* note 252 (explaining that the PIPL and the DSL both expand data localization requirements); *see also* Xiao, *supra* note 251 ("Separately, Chinese regulators on Friday also published new rules requiring companies that process auto data to enhance data security and protect personal information collected from vehicles. The rules require important data, including sensitive military and government locations, to be stored in China, and also set principles for reducing unnecessary collection and sharing of data.").

[255] Samm Sacks & Justin Sherman, *The Global Data War Heats Up*, THE ATLANTIC (June 26, 2019), https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/ ("At issue is how countries view data. Do companies own the information? Does an individual own it? Does a government have access to it? The problem is that governments across China, India, the European Union, Japan, and the United States have philosophical differences on how they view these issues.").

[256] *See id*.; Kateryna Heseleva, Vincent Jerald Ramos, Alan Ichilevici de Oliveira, *Towards a Multilateral Consensus on Data Governance*, G20 INSIGHT (May 29, 2020), https://www.g20-insights.org/policy_briefs/towards-a-multilateral-consensus-on-data-governance/ ("India has advocated for relatively strong localization of personal data, whereas the US, Mexico, and Canada have recently adopted a provision that entirely rejects localization.").

[257] *See* Sherman & Sacks, *supra* note 244 ("The factors that have made China's tech titans successful inside China may not translate well internationally, namely a closed and controlled system. Having lots of data about what Chinese teenagers are buying online, for example, may have little bearing on developing A.I. applications that can compete in the rest of the world—which may be one of the reasons Chinese researchers (like their American counterparts) are using datasets from all over the globe."); *but see Artificial Intelligence and Data Protection in Tension*, CTR. INFO. POL'Y LEADERSHIP (Oct. 2018), https://iapp.org/media/pdf/resource_center/artificial_intelligence_data_protection.pdf (explaining that limiting a data set too much could lead to a biased outcomes from an AI system since there may be biases related to the way that data set was limited initially).

[258] *See* Sacks & Sherman, *supra* note 255 ("India, Europe, and other places will increasingly use data to constrain market access for foreign-incorporated tech firms—for instance, requiring them to store citizens' data within the country, or to not collect it at all—if the U.S. does nothing to dispel the notion that Big Tech cannot be trusted to handle individuals' data in ways that are not exploitative.").

[259] *See id*.

[260] *See id*.; *see also* Mazurek, *supra* note 116 ("The free flow of data across borders is crucial to every stage of the AI life cycle, from its development to deployment and use within the services that sustain global commerce, health care, financial systems and the technologies of the future, just to mention a few. It is clear that the data used for AI purposes often originates from multiple geographically distant sources, which makes large and easy data movements across borders more imperative. Regulations which may at any point limit crossborder

countries may follow China and limit foreign data collection and AI if the United States does not attempt to discredit the idea that U.S. tech giants are free to use anyone's data as they please.[261]

Instead of worrying about the effect of regulation on innovation, China, and to some extent the EU, have chosen to counteract any potential roadblocks by injecting vast sums of money toward incentivizing the creation of AI and developing AI expertise.[262] China has stated that its goal is to be the "primary" leader in AI by 2030, which it articulated in the Next-Generation Artificial Intelligence Development Plan in 2017.[263] In that same plan, China highlighted the need to set global AI standards and cooperate on the international level.[264] In 2019, the Beijing Academy of Artificial Intelligence published AI principles that proclaim similar goals as those given in the AIA—AI should be developed with human benefit as the main goal.[265] Additionally, those principles emphasize the desire for cooperation among national governments in their governance of AI, which will encourage innovation in AI.[266] The Chinese government has been mirroring and keeping pace with the regulations introduced in the EU.[267] While China has left major exceptions to their rules for government oversight, they are outwardly expressing the necessity of cooperating with the EU's approach much more so than the United States.[268]

---

transfers may reduce the insights and other benefits from AI technology."); Masha Borak, *Chinese Tech Firms Can't Win Trust in the West, but the Companies Aren't the Biggest Culprit*, S. CHINA MORNING POST (Apr. 10, 2021), https://www.scmp.com/tech/big-tech/article/3128967/chinese-tech-firms-cant-win-trust-west-companies-arent-biggest ("Unfortunately, the challenge facing Chinese tech companies is not so much about their actual behaviour – whether they have indeed handed over foreign citizen data to the Chinese government – but about how to prove that they have not and will not.").

261 *See* Sacks & Sherman, *supra* note 255; *see also* Nima Elmi, *Is Big Tech Setting Africa Back?*, FOREIGN POL'Y (Nov. 11, 2020), https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/ ("Data colonialism hinders Africans' abilities to develop their own technological innovations based on their indigenous datasets, which have already been exploited by the more established hegemons of the tech world."); *see generally* Paige Leskin, *Here are all the Major U.S. Tech Companies Blocked Behind China's Great Firewall*, BUS. INSIDER (Oct. 10, 2019), https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5.

262 Houser & Raymond, *supra* note 17, at 157–59.

263 *Id.* at 161.

264 Scott J. Shackelford & Rachel Dockery, *Governing AI*, 30 CORNELL J. L. & PUB. POL'Y 279, 311 (2020).

265 *Id.*

266 *Id.*

267 *Id.* at 311–12.

268 *Id.*

An AI race, and the unwillingness of the United States to cooperate with China or the EU, will likely lead to negative outcomes.[269] As it stands now, the AI arms race has no particular objectives or end goals.[270] The overarching objective is seemingly to build an AI system that is the most capable in terms of surveillance capabilities.[271] This is partially the result of thinking about AI development from a military perspective.[272] If AI is constantly considered through a national defense mindset, the result will be a massive surveillance state in each competing country.[273] The EU has prioritized maximizing the social good coming from AI instead of the defense capabilities of the technology.[274] The United States and China should follow suit for the larger social good.[275] Cooperation, instead of international competition, will allow for information exchange and the free movement of knowledgeable AI researchers who can continue to develop AI, all while ensuring that AI is not developed solely for military and surveillance purposes.[276] The consequences of a wait-and-see approach will result in irreversible consequences that the private sector can already foresee.[277]

A chief complaint of Chinese national data policy, even after the enactment of the PIPL, is how limited restraints exist on the ability of the Chinese government to collect and use data freely.[278] The PIPL imposes restrictions on the private collection of data without consent and extends those rules to foreign companies using Chinese citizens' data but grants the Chinese government unrestricted access to that data.[279] The United States does not have the same ability to use privately collected data but can access such data with permission

---

269 Houser & Raymond, *supra* note 17, at 148–49 ("Framing the development of AI as a race will result in losses for everyone.").

270 *Id*.

271 *See id*. ("If advancement succeeds without considering and addressing the potential harms, putting limits on the collection and use of data, and developing international standards, winning the race may lead us straight into a vast surveillance global society.").

272 *Id*. at 160.

273 *Id*. Another result will be cyberwarfare leveraging that surveillance data. Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

274 Houser & Raymond, *supra* note 17, at 161–63.

275 *See id*. ("The motto of the [European] Commission is 'AI for good and for all.' This type of consideration appears secondary in both China and the U.S.").

276 *Id*. at 147–49, 163–64.

277 *Id*.

278 *See* Junck et al., *supra* note 252; Karl Colbary, *Outsourcing the Police: How Reliance on the Private Sector for Law Enforcement Threatens Privacy Legislation Around the World*, 41 NW J. INT'L L. & BUS. 213, 223-24 (2021).

279 Colbary, *supra* note 278, at 226–27, 230–231.

from the companies who collect it.[280] Like China, the United States has similarly lax restrictions on what the government may request from private companies and fewer restrictions on what the private sector can collect.[281] While the United States may use its collected data significantly less frequently than China and is limited in what it can use that information for, the hypocritical pointing of the finger is counterproductive to a cooperative international data regime.[282] The United States is right to admonish the overarching reach of the Chinese government's surveillance state, but those criticisms would hold more weight if the U.S. data privacy laws were more protective of individual rights.

Even after Snowden's disclosure of the PRISM surveillance program by the NSA, the United States continues to collect large amounts of data.[283] As mentioned above, there have been certain executive orders and directives authorizing the collection of bulk data, although those authorities also simultaneously limit the use of that data.[284] While data surveillance requests under the Foreign Intelligence Surveillance Act are subject to review by the United States Foreign Intelligence Surveillance Court, critics point to the lack of independent public advocacy in the courtroom, which results in very few denials of surveillance requests.[285] Furthermore, Executive Order 12333 allows the NSA to collect data, known as signals intelligence, without any oversight from the United States Foreign Intelligence Surveillance Court.[286] The Privacy and Civil Liberties Oversight Board can review the collection, but this board is comprised of five members who each have their own perspectives on data privacy and are not required to advocate for the public's interest in privacy and civil liberties.[287] While Presidential Policy Directive 28 further restricted the ability of intelligence agencies to use bulk data, secret bulk collection of data,

---

[280] *Id*. at 233.

[281] *Id*. at 232–40 ("[U]sers are now paying ISPs for the privilege of having the whole of their internet activity available for sale, and, if history is any guide, law enforcement will be among those lining up to purchase it.").

[282] *See generally* Houser & Raymond, *supra* note 17.

[283] *See* Megan Pugh, *Privacy? What Privacy?: Reforming the State Secrets Privilege to Protect Individual Privacy Rights from Expansive Government Surveillance*, 9 BELMONT L. REV. 265, 274–75, 297–98 (2021) ("In addition to the FISA Amendments Reauthorization Act . . . government surveillance powers have continued to increase through various other enacted legislation, paving the way for more potential surveillance abuses and contributing to the current problem with the state secrets privilege."); *see also* Peter Margulies, *Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 FLA. L. REV. 1045, 1057–60 (2016).

[284] Margulies, *supra* note 283, at 1057–60.

[285] *Id*. at 1111–12.

[286] *Id*. at 1059–60.

[287] *See* Simon Chin, *Introducing Independence to the Foreign Intelligence Surveillance Court*, 131 YALE L.J. 655, 694–96 (2021); *see also* Margulies, *supra* note 283, at 1079.

by itself, could be considered at odds with the objective of the GDPR.[288] There are also growing concerns that United States intelligence agencies, namely the CIA, are not following imposed restrictions.[289]

Additionally, private data collection in the United States continues to act as a surrogate to direct collection by intelligence agencies.[290] Commercial collection of data is still largely unrestricted.[291] While many large tech companies, such as Apple and Microsoft, have publicly opposed complying with government requests for data, many companies are willing to provide information to intelligence agencies.[292] Privacy rights generally point to the Fourth Amendment's restriction on unreasonable searches and seizures as a constitutional basis.[293] However, the Fourth Amendment has so far failed to protect data stored electronically and collected through the internet.[294] The "third-party doctrine," established in *Smith v. Maryland*, states that the Fourth Amendment does not protect data that has been knowingly given to a third party.[295] The Court in *Carpenter v. United States* partially restricted this by stating that law enforcement was required to obtain a warrant for acquiring cell phone location information from a service provider.[296] The Court used a "multi-factor approach" that accounted for the type of data and how that data was collected.[297] The general right to privacy—the right to be left alone—has not been established as a right under the Fourth Amendment.[298] The Supreme Court has been addressing the extension of the Fourth Amendment as it applies to modern technology on an "issue by issue" basis, leaving ambiguity regarding what data is protected from government collection.[299]

In *United States v. Ulbricht*, the Second Circuit held that because Internet Protocol (IP) addresses are non-content information and browsers of the internet

---

288 Linebaugh, *supra* note 189, at 11–12.

289 *Lawmakers Allege 'Secret' CIA Spying on Unwitting Americans*, BBC (Feb. 11, 2022), https://www.bbc.com/news/world-us-canada-60351768.

290 Colbary, *supra* note 278, at 231–40.

291 *Id*. at 240–43.

292 *Id*. at 218–20, 240.

293 *See* Virginia Kozemczak, *Dignity, Freedom, and Digital Rights: Comparing American and European Approaches to Privacy*, 4 CARDOZO INT'L & COMP. L. REV. 1069, 1079–81 (2021).

294 *Id.* at 1091–94.

295 *Id*. at 1089; *see also* Colbary, *supra* note 278, at 218 (citing Smith v. Maryland, 442 U.S. 735, 744–45 (1979)).

296 Colbary, *supra* note 278, at 218 (citing Carpenter v. U.S., 138 S.Ct. 2206, 2221 (2018)).

297 Kozemczak, *supra* note 293, at 1088–90.

298 Colbary, *supra* note 278, at 218.

299 Kozemczak, *supra* note 293, at 1091.

"should know" that their internet service provider receives such "numerical information," IP addresses are therefore not protected by the Fourth Amendment through the "third-party doctrine."[300] The court failed to acknowledge that although IP addresses are "numerical," they can be used to meticulously track a user through cyberspace.[301] Information about certain website visits can be used to determine an individual's daily life just as easily as tracking that individual's location in the outside world.[302] Additionally, the court failed to utilize the reasoning in *Carpenter,* which factored in "whether data collection was hidden, continuous, indiscriminate, and intrusive."[303] It is hard to distinguish exactly what makes the cell phone data tracking in *Carpenter*, which was afforded protection, substantively different from the IP address data in *Ulbricht.*[304] The holding in *Ulbricht* shows that the Fourth Amendment test applied to each new technology at issue will be related to the "reasonable expectation of privacy" and not the more nuanced analysis present in *Carpenter*.[305]

It is important to note the First Amendment implications of the United States' failure to recognize the right to privacy in the digital world.[306] In *Griswold v. Connecticut*, the Court held that "the First Amendment has a penumbra where privacy is protected from governmental intrusion," and "[w]ithout those peripheral rights the specific rights would be less secure."[307] Lack of privacy on the internet leads to self-censorship, has reduced the exercise of First Amendment rights, and has damaged the United States' "reputation as a champion of freedom of expression around the world."[308] This chilling effect on the First Amendment will only continue when the use of AI systems becomes more prevalent in law enforcement and intelligence agencies and the extent of that use becomes public knowledge.[309]

---

[300] *Id*. at 1088–89; *see also* U.S. v. Ulbricht, 858 F.3d 71, 96 (2d Cir. 2017).

[301] Kozemczak, *supra* note 293, at 1090.

[302] *Id*. at 1093.

[303] *Id*. at 1089–90.

[304] *Id*. at 1091–94 ("[The] real issue isn't really about IP addresses, but rather how to handle information which may be non-personal to one party, but which is linked to personal information in the hands of others.").

[305] *Id*. at 1102.

[306] Jennifer M. Paulson, *Cyber Insecurity: Constitutional Rights in The Digital Era*, 41 S. ILL. U. L.J. 261, 277–78 (2017).

[307] *Id*.

[308] *Id*. (citing Global Chilling: The Impact of Mass Surveillance on International Writers, PEN AM. 5 (Jan. 5, 2015), http://www.pen.org/sites/default/files/globalchilling_2015.pdf).

[309] *Id*.

AI decision-making by the government could further exacerbate the deontological and consequentialist problems with collecting data in bulk.[310] "[U]nfettered machine searches would undermine the perception of control that persons abroad have a right to expect . . . [and] unbridled access could cause harm given the amount of incorrect information in searched databases and human analysts' unawareness of or indifference to this problem."[311] Additionally, amassing mass pools of data creates inherent dangers.[312] In the wrong hands, especially when employing the full capabilities of AI, the potential for abuse is astronomical.[313] Even with human oversight, the latent bias and lack of transparency of AI systems have the potential to encroach significantly on human rights norms.[314] This potential for abuse is enough, explicitly so to the EU, to justify constraints on data collection and to protect individual rights such as the right of access, right to be forgotten, and right of portability.[315]

In *Schrems II*, the CJEU raised the EU's concerns about the United States' data collection policies.[316] However, the United States is so far unwilling to enact further oversight and restrictions.[317] Failing to do so has pushed the United States further away from reaching a cooperative data privacy standard that could reduce the effects of the ongoing AI and data race.[318] The United States is doing little to dispel China and the EU's distrust of the lack of a federal data policy.[319] While the EU is setting the current baseline human rights standard, China, and not the United States, has been the first to enact legislation in the direction of

---

310 Margulies, *supra* note 283, at 1075 ("The deontological objection frames privacy as a right that inherently protects the individual against all manner of intrusions, whether by people or machines. In contrast, the consequentialist objection cites the risk that governments, corporations, or other individuals will misuse personal information.").

311 *Id*. at 1107.

312 *See* Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 GEO. L.J. 205, 262–90 (2021) (explaining that the tyrant test, a justification for the fourth amendment, should govern how data is regulated in the United States); Houser & Raymond, *supra* note 17, at 178 ("One particular risk is that AI systems are especially valuable in assisting authoritarian regimes.").

313 *See* Ferguson, *supra* note 312, at 262–90.

314 *See id*.

315 Kozemczak, *supra* note 293, at 1094 ("Many legal scholars agree that the region's support for strong privacy laws emerged from a 'desire to prevent a reoccurrence of population control, similar to that exercised by the Nazis during [World War II].'").

316 *See* Linebaugh, *supra* note 189, at 5–6.

317 Houser & Raymond, *supra* note 17, at 172–73 ("The EU report on AI sums it up as: the U.S. sees AI for profit, China sees it for control, and the EU sees it for society.").

318 *Id*.

319 *Id*. ("While the U.S. fears losing its position as a tech leader and is attempting to roll out 5G as quickly as possible, less attention is being paid to the risks of loss of privacy, automated decision-making, surveillance, and health concerns.").

that standard.[320] It is easy to dismiss the concerns about collecting data in the United States because we do not have the same type of authoritarian government that exists in China.[321] But we need not look far to find examples of oppression against minority groups by the United States.[322] American leadership is not infallible, and appropriate safeguards are necessary to protect the rights of U.S. citizens.[323] The United States should take the lead in protecting human rights violations and champion the rights of citizens to data privacy as the EU has done.[324] Otherwise, we risk losing the international community's trust while China is creating guidelines, like the PIPL, that could enable it to have a better data-sharing relationship with the EU.[325]

V. STEPS MOVING FORWARD FOR THE UNITED STATES

Prioritizing public trust in AI and limiting the harms of AI are imperative objectives for the United States.[326] While there is an unavoidable cost associated with regulation, some argue that the disincentivizing effects and consequent national security implications of AI regulation are likely nonexistent.[327]

---

320 *Id*. at 158 ("Both China and the EU have developed detailed strategic plans for the use and development of AI.").

321 *See* Colbary, *supra* note 278, at 230–31.

322 *See* Justin Worland, *America's Long Overdue Awakening to Systemic Racism*, TIME (June 11, 2020).

323 *See* Ferguson, *supra* note 312, at 262–90.

324 *See* Houser & Raymond, *supra* note 17, at 182–84.

325 *See id*.

326 *See* Crystal Grant & Kath Xu, *Public Trust in Artificial Intelligence Starts with Institutional Reform*, ACLU (Sept. 17, 2021) https://www.aclu.org/news/national-security/public-trust-in-artificial-intelligence-starts-with-institutional-reform/ ("AI might evoke science fiction to some, but it is already being deployed throughout our society in ways that directly impact rights and liberties."); François Candelon et al., *AI Regulation Is Coming*, HARV. BUS. REV. (Sept.-Oct. 2021), https://hbr.org/2021/09/ai-regulation-is-coming ("As companies increasingly embed artificial intelligence in their products, services, processes, and decision-making, attention is shifting to how data is used by the software—particularly by complex, evolving algorithms that might diagnose a cancer, drive a car, or approve a loan.").

327 Will Uppington, *Driving AI Innovation in Tandem with Regulation*, TECHCRUNCH (Oct. 6, 2021), https://techcrunch.com/2021/10/06/driving-ai-innovation-in-tandem-with-regulation/#:~:text=AI%20innovation%20can%20be%20accelerated%20with%20the%20right%20laws&text=Many%20research%20studies%20have%20shown,with%20incentives%20that%20accelerate%20adoption (citing Luke A. Stewart, *The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review*, INFO. TECH. & INNOVATION FOUND. (June 2010)); *see also* Margaret A. Hamburg, *Innovation, Regulation, and the FDA*, N.E. J. MED. (Dec. 2, 2010), https://www.nejm.org/doi/pdf/10.1056/NEJMsa1007467?articleTools=true ("As the FDA set standards for effectiveness, many companies, for the first time, conducted large, randomized, controlled trials to support their claims of efficacy. Major therapeutic breakthroughs ensued, and because of the evidence now required for FDA review, the best drugs, rather than the most aggressively marketed drugs, could rise to the top. In other words, the increasingly rigorous standards of the FDA created the conditions for innovation and progress in the

Conversely, by not regulating AI, the United States is setting up a system that will result in patchwork AI regulation among its states, just like data protection regulation, which will add significant regulatory hurdles to the commercialization of AI systems.[328] The United States should act as a leader by protecting humanitarian interests like the EU proposal seeks to do, rather than letting harmful AI systems run their course to the public detriment before attempting to mitigate their impact.[329] Additionally, the United States should go one step further than the AIA to provide a clear picture of the intellectual property rights surrounding AI as a means of promoting the invention of AI systems.[330]

International cooperation is essential to the responsible development of AI.[331] A uniform international data and AI policy that upholds universal respect for human rights will facilitate the cross-border transfer of data, AI systems, and talented AI researchers and will also ensure that AI develops with a peaceful purpose.[332] An unregulated AI race is detrimental to the benevolent uses of AI, and its only logical end is a mass global surveillance state.[333] The United States must take steps toward international consensus with the EU and China by enacting its own comprehensive laws regarding data and AI.[334]

There are three main approaches the United States could take toward regulating AI.[335] The first would be to regulate a key component of AI: data privacy.[336] The second would be to target specific malicious uses of AI.[337] And

---

pharmaceutical market, and together, American medicine and the FDA have accomplished an enormous amount.").

328 Turner, *supra* note 236, at 3.

329 The United States should implement a system where ethics are embedded into AI from the beginning. Morgenstern, *supra* note 168.

330 *See* Yanisky-Ravid, *supra* note 103.

331 *See* Houser & Raymond, *supra* note 17, at 182–84.

332 *See generally id*.

333 *Id*.

334 *Id*. at 147–49.

335 Bev Townsend, *Decoding the Proposed European Union Artificial Intelligence Act*, AM. SOC. INT'L L. (Sept. 30, 2021), https://www.asil.org/insights/volume/25/issue/20.

336 *Id*.; *see* Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ ("U.S. adults are not convinced they benefit from this system of widespread data gathering. Some 81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits, and 66% say the same about government data collection.").

337 Townsend, *supra* note 335.

a third, which the EU proposal includes, is to provide comprehensive "horizontal regulation of AI systems."[338] This third approach would require more oversight due to its broad reach but would be sufficiently flexible to deal with new AI systems.[339]

Ideally, the United States will adopt some combined form of all three types of regulation, incorporated into a comprehensive and interwoven stratagem similar to what the EU is currently developing.[340] The framework of the GDPR should provide a working model for the United States to create a similar set of federal data privacy regulations.[341] The second approach is already being implemented through agency actions, such as the FTC's guidance, and would be comparable to the current data regulations imposed by agencies.[342] A new agency dedicated to regulating AI could also be a viable option for approaching the everchanging issues produced by AI.[343] The third approach, however, could have significant advantages over the other two, specifically in relation to AI.[344] A comprehensive regulatory framework that issues certifications, similar to the EU proposal, would create a seamless avenue for AI technology to enter use in the United States.[345] "[R]egulatory reform can promote innovation and economic growth by allowing individuals and businesses more freedom to focus their efforts on inventiveness, rather than navigating the overwhelming regulatory road to compliance."[346]

---

[338] *Id*.

[339] *Id*.

[340] *Id*.

[341] A federal U.S. system would not suffer from the same enforcement issues that have plagued the GDPR. *See* Massé, *supra* note 167, at 9–12.

[342] *See* Jillson, *supra* note 29; Klosowski, *supra* note 30.

[343] *See* Rob Toews, *Here Is How The United States Should Regulate Artificial Intelligence*, FORBES (June 28, 2020), https://www.forbes.com/sites/robtoews/2020/06/28/here-is-how-the-united-states-should-regulate-artificial-intelligence/?sh=49bf4ff77821 ("The best way to ensure thoughtful, well-crafted AI policy is through the creation of a federal agency for AI.").

[344] Townsend, *supra* note 335 ("[A] plausible framework should also be nuanced and flexible enough to adapt to, and keep abreast of, the rapidly evolving landscape that is AI development and deployment. Whether the AI Act does this sufficiently in its present form remains to be seen.")

[345] Public trust is essential for the widespread consumption of a product or service. Certain industries, such as air travel, would not be trusted without the high regulation present in the industry. *See* Alan F. T. Winfield & Marina Jirotka, *Ethical Governance is Essential to Building Trust in Robotics and Artificial Intelligence Systems*, PHIL. TRANSACTIONS: MATHEMATICAL, PHYSICAL & ENG'G SCIS. 3–5 (Nov. 28, 2018), https://www.jstor.org/stable/10.2307/26601844.

[346] Brian Kingsley Krumm, *Regulatory Policy in the Trump Era and its Impact on Innovation*, 70 MERCER L. REV. 685, 691 (2019).

The benefits of strong guidelines for the development and use of AI would facilitate further advancement by offering less risk to investors.[347] Explicit national rules for AI implementation will paint a clearer future for AI and promote business confidence in the industry, resulting in growth in this ever-important sector of the economy.[348] The FDA regulatory framework applies a similar methodology for developing pharmaceuticals, and the United States, consequently, is a leader in worldwide drug development.[349] While drug companies are not impervious to public distrust even after drug approval, Americans are nonetheless calling for the FDA's expansion and for greater independence from lobbyists.[350] AI has the potential to create an even greater impact on society than will drugs, and care should be taken accordingly.[351] The increased efficiency, accuracy, and innovation resulting from the widespread use of AI will permeate every aspect of our lives, even without accounting for "general AI."[352] While it is important for the United States to be cautious with regulation, to take this next technological leap, it first must have the mechanisms in place to ensure that AI has a positive effect on society and does not cause irreparable harm.[353]

---

[347] *See* Turner, *supra* note 236.

[348] Krumm, *supra* note 346, at 690–91 ("While there is no proven correlation between decreased regulation and increased economic growth, there is a demonstrated connection between an increase in business confidence and positive economic growth.").

[349] *See* Hamburg, *supra* note 327; Off. of Mgmt & Budget, 2013 Report to Congress on the Benefits and Costs of Federal Regulations and Unfunded Mandates on State, Local, and Tribal Entities (2013), https://obamawhitehouse.archives.gov/sites/default/files/omb/inforeg/2013_cb/2013_cost_benefit_report-updated.pdf (finding the FDA's benefits outweigh its costs).

[350] *See* Claire Felter, *What Is the FDA's Role in Public Health?*, COUNCIL ON FOREIGN RELS. (Sept. 10, 2021), https://www.cfr.org/backgrounder/what-fdas-role-public-health.

[351] *See* Ashley Stahl, *How AI Will Impact The Future Of Work And Life*, FORBES (Mar. 10, 2021, 9:00 AM), https://www.forbes.com/sites/ashleystahl/2021/03/10/how-ai-will-impact-the-future-of-work-and-life/?sh=60ada45a79a3.

[352] *See id*.

[353] *See* MacCarthy, *supra* note 165 ("AI is too important and too promising to be governed in a hands-off fashion, waiting for problems to develop and then trying to fix them after the fact."); B.C. Stahl et al., *Artificial intelligence for human flourishing – Beyond principles for machine learning*, J. BUS. RSCH. 124 (2021), https://reader.elsevier.com/reader/sd/pii/S0148296320307839?token=822ADEDD37BF00F88303610822F8EC9CF85CEAE01DD1B7AA2223FAD273FC9F41EEC797877115BA80E22712BCA77B13E9&originRegion=us-east-1&originCreation=20220109225236 ("The way we deal with the ethics of AI will need to be sensitive to the conceptually challenging and changing nature of the technologies in question and the social perceptions they engender. We should simply not assume that we can provide a permanently stable definition of AI or of the ethical issues related to it. Instead, we need to embrace a world where concepts are changing and contested, where moral preferences change over time, where scientific, media and political discourses dynamically interact and where impacts of new technologies such as AI need to be adequately assessed."); *but see* Chris Reed, *How should we regulate artificial intelligence?*, ROYAL SOC'Y (Aug. 6, 2018), https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2017.0360 ("Good regulation would improve our

CONCLUSION

With the Artificial Intelligence Act, the EU is setting the global standard for AI regulation, as it did with respect to data regulation through the GDPR.[354] The EU's plan for comprehensive regulation of data collection and AI systems is a step in the right direction toward the beneficial development of AI.[355] The United States' hesitation to regulate, mostly stemming from the "AI race" with China, only serves to ensure that a massive surveillance state is realized.[356] For the benefit of humanity, to protect civil liberties, and create an environment for innovation, the United States should seek to promote international cooperation by enacting federal regulations regarding AI and data collection.[357] AI is an integral part of the emergent technological transformation, sometimes referred to as the Fourth Industrial Revolution.[358] The United States must follow the EU to ensure the proper implementation of AI so that the result of that transformation is universal human prosperity.[359]

JOHN HILLMAN

perception of safety, and also our perception that humans remain in control. It could also mitigate any new risks which the use of AI creates. But bad regulation risks stifling the development and implementation of useful AI solutions, perhaps even without improving safety and control. Thus, we need to understand what regulation can and cannot do so that we can shape it appropriately.").

354 *See* Gaumond, *supra* note 31.

355 *See id*.

356 *See* Houser & Raymond, *supra* note 17, at 147–49.

357 *See id*. at 182–84.

358 *Id*.

359 *Id*.