

5-1-2022

## The Need for a Legal Framework to Regulate the Use of Artificial Intelligence

Chris Lewis  
*University of Dayton*

Follow this and additional works at: <https://ecommons.udayton.edu/udlr>



Part of the [Law Commons](#)

---

### Recommended Citation

Lewis, Chris (2022) "The Need for a Legal Framework to Regulate the Use of Artificial Intelligence," *University of Dayton Law Review*. Vol. 47: No. 2, Article 6.  
Available at: <https://ecommons.udayton.edu/udlr/vol47/iss2/6>

This Comment is brought to you for free and open access by the School of Law at eCommons. It has been accepted for inclusion in University of Dayton Law Review by an authorized editor of eCommons. For more information, please contact [mschlange1@udayton.edu](mailto:mschlange1@udayton.edu), [ecommons@udayton.edu](mailto:ecommons@udayton.edu).

---

## The Need for a Legal Framework to Regulate the Use of Artificial Intelligence

### Cover Page Footnote

The author is deeply appreciative to all the members of the *University of Dayton Law Review*, whose combined efforts made this Comment possible, and specifically to Sheldon Linker, who was willing to share his time and technical expertise without hesitation.

# THE NEED FOR A LEGAL FRAMEWORK TO REGULATE THE USE OF ARTIFICIAL INTELLIGENCE

*Chris Lewis, J.D.\**

I. INTRODUCTION .....	286
II. BACKGROUND.....	288
A. HISTORY .....	288
B. HOW DOES ARTIFICIAL INTELLIGENCE WORK? .....	289
C. THE DIFFERENCE BETWEEN ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND DEEP LEARNING .....	290
D. BIG DATA .....	291
E. THE UNITED STATES’S APPROACH TO AI .....	292
III. ANALYSIS.....	294
A. WHY A FRAMEWORK IS NECESSARY.....	294
B. INPUT DATA REGULATION .....	296
C. DATA PRIVACY .....	297
D. THE RIGHT TO BE FORGOTTEN.....	298
E. SYNTHETIC MEDIA .....	299
F. A STRICT LIABILITY REGIME FOR THE USE OF AI.....	302
G. AI AS A JURIDICAL PERSON.....	306
H. RESEARCH AND DEVELOPMENT IN LIGHT OF REGULATION .. .....	306
IV. CONCLUSION .....	307
APPENDIX A.....	308
CHATS WITH ARTIFICIAL INTELLIGENCE BOTS.....	308
Transcript 1: Questions on Synthetic Media and Deepfakes.....	308
Figure A1 depicts the messages with the Kuki AI Chatbot on October 27, 2020, at 10:00 PM.....	310
Figure A2 depicts the messages with the Emerson AI on March 19, 2021, at 12:38 PM .....	311

*“[They] were so preoccupied with whether or not they could,  
they didn’t stop to think if they should.”<sup>1</sup>*

---

\* Chris Lewis is a 2022 graduate of the University of Dayton School of Law. He is deeply appreciative to all the members of the Dayton Law Review whose combined efforts made this Comment possible, and specifically to Sheldon Linker, who was willing to share his time and technical expertise without hesitation.

<sup>1</sup> JURASSIC PARK (Universal Pictures 1993).

## I. INTRODUCTION

That quote was originally about scientists creating man-eating dinosaurs in the film *Jurassic Park*, but it can be applied equally well to the use of artificial intelligence by businesses. Artificial intelligence (“AI”) is an unapproachable topic to many. Big data, machine learning, neural networks, algorithms, deep learning, and the internet of things—there are so many technical buzzwords that it can be hard to make sense of it all.<sup>2</sup> The portrayal of AI in the media has been of little help in improving the public’s understanding of AI. The media usually depicts AI that is capable of answering any question or presents a dystopian society where AI attempts to destroy humanity.<sup>3</sup> It is important to recognize the reality of AI and its legal and societal implications, even though the elusive capabilities of AI may blur the lines between fiction and reality.<sup>4</sup> In the simplest sense, AI is the ability of a machine to convert inputted data into recognizable patterns and/or then use those patterns to formulate decisions.<sup>5</sup> These decisions could be anything, including how to traverse an environment, what font to use to maximize sales, or even something as complicated as predicting tomorrow’s weather.

Businesses are at the vanguard of developing and implementing AI. The United States government is not far behind though and is already positioning itself to respond to the widespread adoption of AI.<sup>6</sup> There have been numerous proposals, initiatives, memorandums, and hearings in Congress.<sup>7</sup> Despite these efforts, however, the creation of a standardized regulatory framework governing the use of AI has yet to be implemented.<sup>8</sup>

In the meantime, unregulated AI is beginning to run amok in society. In 2016, Microsoft put an AI chatbot on Twitter, nicknamed Tay, designed to mimic a stereotypical high school girl; Microsoft hoped that Tay would discover patterns in language through “her” interactions with Twitter users and then utilize similar patterns to create her own tweets.<sup>9</sup> By the end of Tay’s first day online, she had transformed from a “hip” teenage girl into a racist

---

<sup>2</sup> 50 AI Terms Every Beginner Should Know, TELUS INT’L. (Mar. 1, 2021), <https://lionbridge.ai/articles/50-beginner-ai-terms-you-should-know/>.

<sup>3</sup> See e.g., THE HITCHHIKER’S GUIDE TO THE GALAXY (Touchstone Pictures 2005); TERMINATOR (Cinema ‘84 1984).

<sup>4</sup> See An Open Letter to the United Nations Convention on Certain Conventional Weapons (Aug. 20, 2017) (on file with the Future of Life Institute).

<sup>5</sup> Ed Burns et al., *What is artificial intelligence (AI)?*, TECHTARGET, <https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence> (Feb. 2022).

<sup>6</sup> See generally Memorandum from Russel T. Vought, Dir. of the Off. of Mgmt. & Budget, on Guidance for Regulation of Artificial Intelligence Applications to Heads of Exec. Dep’ts & Agencies 1 (Nov. 17, 2020) [hereinafter OMB Memo]; Exec. Order No. 13,859, 84 Fed. Reg. 3967 (Feb. 11, 2019).

<sup>7</sup> 784 Fed. Reg. 3967.

<sup>8</sup> Andrew Burt, *New AI Regulations Are Coming. Is Your Organization Ready?*, HARV. BUS. REV. (Apr. 30, 2021), <https://hbr.org/2021/04/new-ai-regulations-are-coming-is-your-organization-ready>.

<sup>9</sup> Oscar Schwartz, *In 2016, Microsoft’s Racist Chatbot Revealed the Dangers of Online Conversation*, IEEE SPECTRUM (Nov. 25, 2019), <https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation>.

bigot.<sup>10</sup> Tay tweeted things such as “I [expletive removed] hate feminists and they should all die and burn in hell,” and “Bush did 9/11 and Hitler would have done a better job.”<sup>11</sup>

Unfortunately, tweets are the least of the worries as AI has been implemented into more life-threatening scenarios. An unfortunate mishap occurred in May 2016 when an AI-programmed Tesla failed to make the obvious distinction between a clear spring sky and the side of a white semi-truck trailer, resulting in the vehicle’s driver’s death.<sup>12</sup> In 2013, IBM partnered with the University of Texas M. D. Anderson Cancer Center to employ Watson, an advanced IBM computer and operating system which utilizes AI methodologies, to diagnose and provide treatment recommendations for patients with cancer.<sup>13</sup> Unfortunately, after a \$62 million investment, Watson was not very good at its job and frequently gave incorrect and unsafe treatment recommendations, which forced the program to be scrapped.<sup>14</sup>

The myriad of dangers and uncertainties regarding the use of AI, as illustrated above, necessitates prompt congressional action to ensure the development and adoption of AI do not remain unstructured. If Congress refrained from acting on AI regulation, a cacophony of inconsistent regulation would be produced from the court system and state legislatures. AI is a technology that will likely become integral to our daily life and allowing the haphazard development of the laws governing it is certain to cause problems in the future. Accordingly, this Comment will address the most pressing issues posed by AI use and present ideas that can be incorporated into a legal framework to resolve such issues.

AI is not a standalone issue; it is inextricably linked with consumer data and privacy, and therefore, any approach to AI regulation will necessitate the creation of laws governing these issues.<sup>15</sup> Congress’s approach to the regulation of AI needs to address AI systems in their entirety. At the outset, the data that is fed into AI systems should be required to meet certain minimum standards to ensure accurate results. Congress must heighten protections regarding consumer data used and processed by AI. Additionally,

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> Danny Yadron & Dan Tynan, *Tesla driver dies in first fatal crash while using autopilot mode*, GUARDIAN (June 30, 2016, 7:14 PM), <https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk>; *Collision Between Car Operating with Partial Driving Automation and Truck-Tractor Semitrailer*, NAT’L TRANSP. SAFETY BD., <https://www.nts.gov/investigations/Pages/HWY19FH008.aspx> (Mar. 15, 2021, 3:39 PM).

<sup>13</sup> Eliza Strickland, *How IBM Watson Overpromised and Underdelivered on AI Health Care*, IEEE SPECTRUM (Apr. 2, 2019), <https://spectrum.ieee.org/biomedical/diagnostics/how-ibm-watson-overpromised-and-underdelivered-on-ai-health-care>.

<sup>14</sup> *Id.*

<sup>15</sup> Bev Townsend, *Decoding the Proposed European Union Artificial Intelligence Act*, AM. SOC’Y INT’L L. (Sept. 30, 2021), <https://www.asil.org/insights/volume/25/issue/20>.

AI systems that exhibit advanced person-like displays of intelligence should be considered juridical persons, acting as agents of whatever entity is presently holding that AI system out for engagement with the public. This would allow entities involved with AI systems to easily determine liability and create an economic incentive for entities to use AI responsibly.

At this time, traditional mental state requirements are inapplicable to AI because AI does not currently possess the ability to form human-like intent.<sup>16</sup> Thus, AI liability should be on an effects-only/strict liability basis. Furthermore, the creation of synthetic media by AI should be addressed specifically in order to limit the serious risk of harm they pose to society. Lastly, as the United States Office of Management and Budget (“OMB”) acknowledges, there should be research and development exceptions for AI to encourage investment and innovation.<sup>17</sup> If congressional legislation is going to be effective in addressing the problems caused by AI, as well as simultaneously fostering AI’s growth, Congress should adopt a framework incorporating these characteristics.

## II. BACKGROUND

### A. HISTORY

The notion of AI has been around for thousands of years. Homer first depicted AI in the *Iliad* in the eighth century B.C.E.<sup>18</sup> In the epic, the god Hephaestus creates “attendants made of gold, which seemed like living maidens.”<sup>19</sup> Although there is no reference to machine learning or neural networks, this imitation of human thought captures the essence of AI. But AI, in its more modern sense, dates back to the 1950s.<sup>20</sup> In 1955, a Dartmouth mathematics professor named John McCarthy declared that “every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.”<sup>21</sup> Following this, in 1956, the term “artificial intelligence” was officially coined.<sup>22</sup> Implementation of AI, however, was held back due to lack of funding, slow computer-processing speeds, and limited computer storage capacity.<sup>23</sup>

---

<sup>16</sup> See F. Cuzzolin et al., *Knowing me, knowing you: theory of mind in AI*, 50 PSYCH. MED. 1057 (2020), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7253617/>.

<sup>17</sup> OMB Memo, *supra* note 6, at 7.

<sup>18</sup> *Portrayals and perceptions of AI and why they matter*, THE ROYAL SOC’Y, 7 (Nov. 2018), <https://royalsociety.org/-/media/policy/projects/ai-narratives/AI-narratives-workshop-findings.pdf>.

<sup>19</sup> *Id.*

<sup>20</sup> John McCarthy et al., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, AI MAG., (Aug. 2006), at 12.

<sup>21</sup> *Id.*

<sup>22</sup> Rockwell Anyoha, *The History of Artificial Intelligence*, HARV. UNI.: SCIENCE IN THE NEWS (Aug. 28, 2017), [sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/](http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/).

<sup>23</sup> *Id.*

Decades later, some would say the idea of replicating human intelligence has been achieved.<sup>24</sup> Today, AI's constraints have been greatly reduced by the advancement of technology.<sup>25</sup> Moore's Law, which predicted the exponential growth in the processing power of computers, proved to be accurate, and the world has seen significant growth in computers' computational power.<sup>26</sup> Some of the largest businesses and governments in the world have begun to invest heavily in AI systems.<sup>27</sup> As a result, AI can now recall and analyze data at speeds fast enough to make it useful in everyday society.

### B. HOW DOES ARTIFICIAL INTELLIGENCE WORK?

An AI system works by taking input data and running it through a series of algorithms in order to make a prediction, solve a problem, interpret conditions, or actuate something, such as autopilot.<sup>28</sup> These algorithms are mathematical and logic commands and can be thought of as step-by-step instructions on how to process the input data.<sup>29</sup> After the data is run through the algorithms, the model generates an end result.<sup>30</sup> Traditionally a human reviewed this result for its accuracy, but some more advanced AI systems are now capable of machine learning, a process used to analyze the accuracy of the result without human assistance.<sup>31</sup> Based on the results of the analysis, the AI system will go back and adjust the relevancy it gives to certain aspects of the input data or reorganize the steps of the algorithm in order to create a more successful prediction.<sup>32</sup> The key to the success of an AI system employing machine learning is the development of this feedback loop, which leads to the constant improvement of the AI's prediction.<sup>33</sup>

---

<sup>24</sup> *Artificial Intelligence News: Latest Articles, Developments & Examples*, BUS. INSIDER, <https://www.businessinsider.com/artificial-intelligence> (last visited May 17, 2022).

<sup>25</sup> Anyoha, *supra* note 22.

<sup>26</sup> Editors of Encyc. Britannica, *Moore's Law*, BRITANNICA, <https://www.britannica.com/technology/Moores-law> (last visited May 17, 2022). Moore's law states that the number of transistors on a microchip doubles every two years, and the cost of computers is halved. Carla Tardi, *Moore's Law*, INVESTOPEDIA, <https://www.investopedia.com/terms/m/mooreslaw.asp> (Feb. 23, 2021).

<sup>27</sup> Ljubinko Zivkovic, *Investments by Tech Giants In Artificial Intelligence is Set to Grow Further*, UNITE.AI <https://www.unite.ai/the-investments-of-tech-giants-in-artificial-intelligence-is-set-to-grow-further/> (Oct. 17, 2020); Tardi, *supra* note 26.

<sup>28</sup> Stephen F. DeAngelis, *Artificial Intelligence: How Algorithms Make Systems Smart*, WIRED, <https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/> (last visited May 17, 2022).

<sup>29</sup> *Id.*

<sup>30</sup> *How Does AI Work*, STRATEGIC CONTACT, <https://www.strategiccontact.com/blog/2018/07/how-does-ai-work/> (last visited May 18, 2022).

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> Natalie Fletcher, *Closing The Loop: How Feedback Loops Help To Maintain Quality Long-Term AI Results*, CLARIFAI (May 24, 2019), <https://www.clarifai.com/blog/closing-the-loop-how-feedback-loops-help-to-maintain-quality-long-term-ai-results>.

C. *THE DIFFERENCE BETWEEN ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND DEEP LEARNING*

AI is the incorporation of analysis usually associated with human intelligence in machines.<sup>34</sup> As a hypothetical example, imagine an algorithm receiving input data from a camera that is observing students in a classroom. If the algorithm could detect what gender the students are and what color shirt they have on, it would be considered an AI. This is because identifying gender and color are abilities traditionally associated with human reasoning.

Machine learning is a more advanced subsection of AI.<sup>35</sup> Machine learning is the ability of computer systems to “learn” based on inputted data.<sup>36</sup> In the prior example, the AI system lacked machine learning capabilities. Although the AI could discern the given characteristics of the people in the room, the result was static, meaning the AI could not attempt to improve or judge the accuracy of its predictions. Imagine, now, that in addition to the camera recording all of the characteristics, the AI system stores months and months of this data. In order to make the jump from a static AI to an AI system that utilizes machine learning, the system has to have some method of using its experiences to improve its outcomes, such as being fed training data, which includes both input variables and the correct prediction or result.<sup>37</sup> Like the linear prediction equation  $y=mx+b$ , a machine learning system would work by taking these two variables, giving them various weights, and then seeing how these different combinations affect the prediction of someone’s gender.<sup>38</sup> Machine learning can be thought of as operating like a syllogism. The system repeatedly reaches a conclusion based on premises and then repeats this process thousands of times until the most accurate results are reached. During this repetitious process, the machine is essentially evaluating the validity of the decision-making criteria to see which ones are most supportive of the goal of the system.<sup>39</sup>

Just as machine learning is a subset of AI, deep learning is a subset of machine learning.<sup>40</sup> Deep learning goes a step further than machine learning by creating neural networks between the variables to assist in the prediction process.<sup>41</sup> Whereas a machine learning system views the variables independently of one another, a deep learning system connects the dots

---

<sup>34</sup> Michael J. Garbade, *Clearing the Confusion: AI vs Machine Learning vs Deep Learning Differences*, TOWARDS DATA SCI. (Sept. 14, 2018), <https://towardsdatascience.com/clearing-the-confusion-ai-vs-machine-learning-vs-deep-learning-differences-fce69b21d5eb>.

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> *Machine Learning*, IBM CLOUD LEARN HUB (July 15, 2020), <https://www.ibm.com/cloud/learn/machine-learning>.

<sup>39</sup> *Id.*

<sup>40</sup> Garbade, *supra* note 34.

<sup>41</sup> *Basics of Deep Learning and Neural Networks*, BLOCKGENI (Mar. 11, 2021), <https://blockgeni.com/basics-of-deep-learning-and-neural-networks/>.

between the variables to see if patterns exist and then uses those patterns to make predictions.<sup>42</sup> This process is similar to how the human brain makes decisions. The brain does not predict gender based on someone's height, then predict gender based on their weight, and then throw the two predictions together to come to a conclusion. The human brain would predict someone's gender based on *the relationship* between those two facts. The main difference is that a deep learning AI system can draw connections between hundreds of variables at a time, while the human mind is limited to drawing connections between only a handful of variables to make a prediction.<sup>43</sup>

#### D. BIG DATA

AI is becoming increasingly associated with the concept of big data. In simple terms, big data equates to extremely large amounts of information.<sup>44</sup> In the AI industry, it is denoted by volume, velocity, and variety.<sup>45</sup> Volume is the amount of data there is, velocity is a measure of how fast the data is being collected and recorded, and variety is the format of the data.<sup>46</sup> Regular data becomes big data when it becomes too unwieldy to analyze under traditional means.<sup>47</sup>

There has been a recent increase in the amount of big data being generated due to the internet of things ("IoT").<sup>48</sup> The IoT is a network of devices capable of generating data through its various sensors.<sup>49</sup> These devices could be in the form of a Google Home listening in the background, your phone reporting your internet searches, or a smartwatch keeping track of your vitals.<sup>50</sup> These data harvesting tools are constantly "listening in" and keeping track of what is happening around them.<sup>51</sup> Since these devices are connected to the internet, they can send the information they collect in real-time to the businesses that own or control them.<sup>52</sup> The amount of information produced by these IoT devices is often large, variable, and generated at a very rapid pace.<sup>53</sup> Thus, as a direct result of the IoT, there has been a substantial increase in big data in recent years.<sup>54</sup> All this data has to be processed if they

---

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Big Data What it is and why it matters*, SAS INST., [https://www.sas.com/en\\_us/insights/big-data/what-is-big-data.html](https://www.sas.com/en_us/insights/big-data/what-is-big-data.html) (last visited May 18, 2022).

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*

<sup>48</sup> Pankaj Mudholkar & Megha Mudholkar, *Internet of Things (IoT) and Big Data: A Review*, 8 INT. J. OF MGMT., TECH., AND ENG'G 5001, 5003 (2018).

<sup>49</sup> *Id.* at 5001.

<sup>50</sup> *Id.* at 5004–06.

<sup>51</sup> Grant Clauser, *Amazon's Alexa Never Stops Listening to You. Should You Worry?*, N.Y. TIMES: WIRECUTTER (Aug. 8, 2019), <https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/>.

<sup>52</sup> *Id.*

<sup>53</sup> Mudholkar & Mudholkar, *supra* note 48, at 5001.

<sup>54</sup> *Id.* at 5003.

are going to have any value to the businesses and governments that collect them. Since traditional methods are ineffective at analyzing such large amounts of information, businesses have turned to AI to convert all those data into useful decision points.<sup>55</sup> The relationship between big data and AI is symbiotic: without AI, big data is useless because such enormous volumes of data would not be able to be analyzed in the first place; without big data, AI is pointless because AI's value is in discovering patterns that humans cannot, and big data provides the information from which these patterns are drawn.<sup>56</sup> This rampant commoditization of consumer information raises serious invasion of privacy concerns. Oftentimes, the consumer's personal information is not just used by the company that initially generates that data. It is usually sold downstream too, changing hands multiple times.<sup>57</sup> Prime examples of this are those creepy advertisements that seem to know just what someone is thinking about buying before they mention it to anyone or even type in a search.

In 2018, California passed the California Consumer Privacy Act ("CCPA"), the most robust set of data privacy regulations in the country.<sup>58</sup> The CCPA included: the right of a person to know what data a business is collecting and how it is being used and shared, the right to delete personal information collected from them, the right to opt-out of the sale of their personal information, and the right to non-discrimination for exercising rights under the CCPA.<sup>59</sup> Some companies like Facebook and Google have self-regulated some aspects of their data use voluntarily, but without putting concrete laws on the books, Congress is leaving the fox to guard the henhouse.<sup>60</sup> Selling data is big business; the data brokerage industry's estimated value is near \$200 billion.<sup>61</sup> Self-regulation can work in some instances, but the monetary incentives to abuse consumer data will not be ignored by capitalists and should not be ignored by lawmakers either.

#### E. THE UNITED STATES'S APPROACH TO AI

Donald Trump issued an executive order ("EO") that called for the OMB to develop plans for the utilization of AI in the workforce, the creation of standards for AI use, and government investment in AI technology.<sup>62</sup> In the EO, the OMB was instructed to "consider ways to reduce barriers to the

---

<sup>55</sup> *Big Data and Artificial Intelligence: How They Work Together*, MARYVILLE UNIV., <https://online.maryville.edu/blog/big-data-is-too-big-without-ai/> (last visited May 18, 2022).

<sup>56</sup> *Id.*

<sup>57</sup> *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE@WHARTON (Oct. 28, 2019), <https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/>.

<sup>58</sup> *See generally* CAL. CIV. CODE DIV. 3, PT. 4, § 1.81.5.

<sup>59</sup> *See generally id.*

<sup>60</sup> *Your Data Is Shared and Sold . . . What's Being Done About It?*, *supra* note 57.

<sup>61</sup> David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, L.A. TIMES (Nov. 5, 2019, 5:00 AM), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

<sup>62</sup> OMB Memo, *supra* note 6.

use of AI technologies in order to promote their innovative application while protecting civil liberties, privacy, American values, and United States economic and national security.”<sup>63</sup> The approach that the Trump administration was detailing was one of minimal involvement: the government should not intervene regarding AI use unless fundamental American liberties are at stake.<sup>64</sup>

Subsequently, the OMB released a draft of ten proposed rules to guide federal agency regulation of AI.<sup>65</sup> Borrowing the definition from the John S. McCain National Defense Authorization Act for Fiscal Year 2019, the OMB defined AI as:

- (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
- (2) An artificial system developed in computer software, physical hardware, or another context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
- (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
- (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.
- (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.<sup>66</sup>

Since OMB has oversight authority over all of the other federal agencies, any agency regulation governing the use of AI under this definition will have to be in accordance with the final rules drafted by the OMB.<sup>67</sup> The proposed guidelines “set[] out policy considerations that should guide, to the extent permitted by law, regulatory and non-regulatory approaches to AI applications developed and deployed outside of the Federal government.”<sup>68</sup> The ten proposed principles for guiding regulatory agencies were: promotion of public trust in AI, public participation in the rulemaking process, scientific

---

<sup>63</sup> Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019).

<sup>64</sup> Joel Nantais, *Federal Government Regulation of AI: Here comes big brother? Or finally our savior?*, TOWARDS DATA SCI. (Jan. 20, 2020), <https://towardsdatascience.com/federal-government-regulation-of-ai-4fa08b7bd99a>.

<sup>65</sup> *Id.* See generally OMB Memo, *supra* note 6.

<sup>66</sup> OMB Memo, *supra* note 6, at 1 n.2 (quoting 10 U.S.C. § 2358).

<sup>67</sup> Nantais, *supra* note 64.

<sup>68</sup> OMB Memo, *supra* note 6, at 1.

integrity and information quality, regulation based on risk assessment and management, cost/benefit analysis of proposed AI regulation, the flexibility of AI regulations, fairness of AI regulations, transparency and disclosure of AI use, safety and security of AI systems, and interagency coordination of AI regulation.<sup>69</sup> Additionally, the Memo detailed non-regulatory approaches executive agencies should take, including establishing best practice standards for the use of AI, encouraging waivers and exceptions to existing innovation to foster growth, allowing access to federal data sets, and establishing a consistent approach to AI across different regulatory agencies.<sup>70</sup> In theory, federal agencies will be required to consider the guiding principles established in the Memo when creating regulations regarding the use of AI in private industries. On November 17, 2020, the final version of the OMB memo was released, consisting of the same, ten guiding principles for the development of AI regulation detailed in the draft memo.<sup>71</sup>

The OMB approach emphasizes the importance of reducing barriers to the use of AI technologies to avoid stifling innovation in the nascent field.<sup>72</sup> The government has taken a hands-off approach to AI regulation in the hopes that American businesses will capitalize on the freedom to innovate, develop, and implement AI that will benefit society.<sup>73</sup> The government's laissez-faire approach is conducive to early growth because there are no restrictions, but such freedom will be a recipe for disaster down the road. Already, certain states have begun implementing more restrictive AI standards, such as California's CCPA.<sup>74</sup> If this trend continues, an unstructured regulatory framework in the U.S. will emerge that will lack uniform national standards and consist instead of independently adopted regulations among individual states. Such a disconnected regulatory framework will have the opposite effect of promoting growth in the long run. As companies develop AI, they will be hindered in their implementation as they attempt to adjust to inconsistent regulation throughout the United States.

### III. ANALYSIS

#### A. WHY A FRAMEWORK IS NECESSARY

Getting the United States government to address a problem can be arguably one of the slowest processes imaginable. As outlined by the OMB, even they have come to see that there is a pressing need to guide the

---

<sup>69</sup> *Id.* at 3–7.

<sup>70</sup> *Id.* at 7–8.

<sup>71</sup> OMB Memo, *supra* note 6, at 3–10.

<sup>72</sup> OMB Memo, *supra* note 6, at 2, 8.

<sup>73</sup> *Id.*

<sup>74</sup> *Legislation Related to Artificial Intelligence*, NAT'L CONF. OF STATE LEGIS., <https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx> (Jan. 5, 2022); CAL. CIV. CODE DIV. 3, PT. 4. § 1.81.5.

development of AI use in the United States.<sup>75</sup> Although there are benefits to giving tech companies carte blanche over AI development, the day is inevitable when society will have to reckon with the problems that the capabilities of AI will inevitably cause. Prompt congressional action is needed in order to ensure that AI use is integrated into society in a way that prevents these future harms rather than solely mitigating them.

At the turn of the twentieth century, unregulated meatpacking in the United States led to a deluge of problems. Once these problems were exposed in the book, *The Jungle* by Upton Sinclair, Congress was forced to act swiftly to deal with the public backlash.<sup>76</sup> Rather than wait and take such a reactionary approach, it is necessary to set up a legal framework as quickly as possible in order to guide the development of AI. This legal framework may benefit from a phased implementation approach. This approach will allow the legislature to tailor the regulation to AI as it develops and people innovate its use. A phased implementation of AI law would likely more accurately reflect the natural development of societal attitudes towards new technology.<sup>77</sup> Perceptions change, unexpected events arise, and nobody truly knows how quickly technology will transform or how innovative the development will be.

There are some benefits of the carte blanche system the OMB proposes that are worth recognizing.<sup>78</sup> Companies acting with no restrictions are free to pursue AI use to the fullest.<sup>79</sup> With no restrictions, companies would likely invest in rapid development and rollouts. Furthermore, the absence of a national legal framework allows the legal and judicial systems to apply a trial-and-error method. Courts and legislatures all over the country will make laws and rulings on some aspects of AI use. These laws and rulings will inevitably vary from state to state, and this lack of uniformity will provide an opportunity to assess which approaches work best.

Although this approach may sound appealing, it would not be an effective reality. In the course of a single year, twenty-five states introduced legislation to regulate AI.<sup>80</sup> None of their approaches were exactly alike. AI is a technology that is ill-suited to such varying regulatory approaches.<sup>81</sup> Business is no longer confined by brick-and-mortar stores mainly relegated to one state. The rise of the digital era has created an e-commerce

---

<sup>75</sup> See generally OMB Memo, *supra* note 6, at 1.

<sup>76</sup> See UPTON SINCLAIR, *THE JUNGLE* (1906); 21 U.S.C. § 601–95 (1906).

<sup>77</sup> William B. Cassidy, *ELD enforcement to be 'phased in' through April 2018*, J. COM. (Aug. 28, 2017, 12:07 PM), [https://www.joc.com/regulation-policy/transportation-regulations/us-transportation-regulations/eld-enforcement-be-phased-through-april-2018\\_20170828.html](https://www.joc.com/regulation-policy/transportation-regulations/us-transportation-regulations/eld-enforcement-be-phased-through-april-2018_20170828.html).

<sup>78</sup> OMB Memo, *supra* note 6, at 7–8.

<sup>79</sup> John Pavlus, *AI is moving too fast, and that's a good thing*, FAST CO. (Dec. 3, 2019), <https://www.fastcompany.com/90429993/ai-is-moving-too-fast-and-thats-a-good-thing>.

<sup>80</sup> *Your Data Is Shared and Sold . . . What's Being Done About It?*, *supra* note 57.

<sup>81</sup> Mark MacCarthy, *AI needs more regulation, not less*, THE BROOKINGS INST. (Mar. 20, 2020), <https://www.brookings.edu/research/ai-needs-more-regulation-not-less/>.

environment where nearly every business engages in markets all across the country. It would be an impermissible financial and technological burden on businesses to force them to tailor their AI systems to the whims of every state legislature or court system in the land. Algorithms are not always easily understood or adjusted, and forcing companies to make numerous derivative forms to meet the varying standards of each state poses serious threats to their overall efficiency and interoperability.<sup>82</sup> It is imperative that the federal government develops a national AI framework, and all state regulations are preempted to avoid the problems created by unstructured technological development.

### B. INPUT DATA REGULATION

Congress needs to adopt a reasonable person standard for input data used by AI systems. A major hazard of input data is that bias in the collection process can lead to skewed data, which ultimately leads to biased final conclusions of the AI output.<sup>83</sup> IBM's Watson's fatal flaw was inadequate input data, leading to drastic inconsistencies.<sup>84</sup> Although Watson had advanced natural language processing skills, the medical records it gathered data from had reports that contained missing information, were written down in ambiguous ways, and were out of chronological order.<sup>85</sup> Simple oversights like this are easy enough for humans to work through, but they pose serious hurdles to AI trying to extract data for decision-making.<sup>86</sup> AI is often not able to identify these mistakes and simply takes the data as it is presented.

Setting a concrete minimum standard for data quality and quantity would likely be impossible due to the complexities of AI and the problems it is trying to address.<sup>87</sup> A skilled AI model likely needs less data than a crude one. Data sets for AI models predicting your likelihood of hereditary diseases should be much larger when compared to data sets for AI that predict something like what your favorite ice cream flavor will be. In addition, things such as the number of the input variables, the range of outputs you are looking at, and the quality of the data you are using play a part in how much data is necessary to create the AI model.<sup>88</sup> The information the AI model is using

---

<sup>82</sup> Chris Marden & Rob Nicholls, *Interoperability: A solution to regulating AI and social media platforms*, SOC'Y FOR COMPUT.S' AND L., <https://www.scl.org/articles/10662-interoperability-a-solution-to-regulating-ai-and-social-media-pla> (last visited May 18, 2022).

<sup>83</sup> James Manyika et al., *What Do We Do About the Biases in AI?*, HARV. BUS. REV. (Oct. 25, 2019), <https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai>.

<sup>84</sup> Strickland, *supra* note 13.

<sup>85</sup> *Id.*

<sup>86</sup> *Id.*

<sup>87</sup> Jason Brownlee, *How Much Training Data is Required for Machine Learning?*, MACH. LEARNING MASTERY, <https://machinelearningmastery.com/much-training-data-required-machine-learning/> (May 23, 2019).

<sup>88</sup> *Id.*; Nick Heath, *What is AI? Here's everything you need to know about artificial intelligence*, ZDNET (July 23, 2021), <https://www.zdnet.com/article/ai-for-business-whats-going-wrong-and-how-to-get-it-right/>.

has to be broad enough to cover the wide range of possibilities that it will encounter when it operates in the real world. Furthermore, where applicable, the data used by AI should be required to meet certain standards for data quality.<sup>89</sup> Whether or not there is sufficient data quality should be analyzed based upon the reliability of the data collection method, as well as the lateral and vertical scope of the data, with lateral scope being the quantity and diversity of the data and vertical scope being the period of time or intervals over which the data was gathered.

Since a bright-line standard for judging data quality is impractical, courts should weigh a number of factors in determining whether the input data is reasonably sufficient, including: (1) the complexity of the problem; (2) the sophistication of the AI model; (3) and the quality of the data, where the trustworthiness of the data defines quality points both laterally and vertically.<sup>90</sup> By adopting a factor test for input data quality, Congress can avoid problems, such as discrimination and poor predictions, which result from biased or inadequate data.

### C. DATA PRIVACY

Congress needs to adopt new industry standards for data collection within the terms and conditions of agreements. In the digital world, terms and conditions agreements have become ubiquitous. They are associated in some way with almost every online product, and because of this, most consumers do not pay a second thought to them.<sup>91</sup> Oftentimes buried deep within these agreements are the conditions regarding data collection. Rather than allow companies to obfuscate the consumer data collection terms deep in the heart of the terms of service, companies should be forced to present them in an easily understandable format with their own required mark or signature of consent. When coupled with the easily understandable format, the terms concerning data privacy should be isolated from the terms of service that pertain to the rest of the agreement. Separating the terms of service for data collection from the regular terms of service will allow consumers to be easily informed about what is going on with their data. Furthermore, it still allows companies to gather information.

The main goal of this proposed approach is transparency. Although this approach would potentially face backlash from tech companies, it is necessary to protect consumer information. The separate form should include, in easily understandable terms: (1) what data is being collected; (2)

---

<sup>89</sup> Wilson Pang, *How to Ensure Data Quality for AI*, INSIDEBIGDATA (Nov. 17, 2019), <https://insidebigdata.com/2019/11/17/how-to-ensure-data-quality-for-ai/>; Heath, *supra* note 88.

<sup>90</sup> See Brownlee, *supra* note 87.

<sup>91</sup> David Berreby, *Click to agree with what? No one reads terms of service, studies confirm*, GUARDIAN (Mar. 3, 2017, 8:38 PM), <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>.

how the data is being collected; (3) who is collecting the data; (4) whether the data is sold to a third party, and, if the data is sold to a third party, who that third party is; and (5) whether the information can be traced to that individual user. This approach aims not to stifle the collection of big data but rather to give consumers the information they need to make informed decisions about their information. Additionally, Congress should give an individual the right to be able to “opt-out” of the data collection and still use the product. In the event an individual wishes to exercise this right, regulation should protect the individual from reprisals aimed at discouraging opting out of data collection.

When it comes to the final output of their data, consumers should have a right to transparency in matters connected to personal health and wellbeing.<sup>92</sup> To illustrate, consider the following scenario. If a health insurance company took data on their consumers, it could tell that a certain consumer is at an extremely high risk of certain cancers. The insurance company could then use that information to skyrocket the price of that person’s insurance plan. The insurance company would be under no obligation to inform the person that they are highly susceptible to certain cancers, and the person would continue their life in total ignorance of the health risks hanging over their head. This raises both legal and ethical concerns and shows why transparency is so crucial in company-consumer data relationships, especially in the healthcare industry. Although consumers whose data is being used should not be entitled to all the information that results from the AI model using their data, the consumers should at least be entitled to their individual results computed by the AI system if the output has anything to do with the health or safety of the individual.

#### D. THE RIGHT TO BE FORGOTTEN

In 2018, the European Union passed the General Data Protection Regulation (“GDPR”), which formalized an individual’s “right to be forgotten.”<sup>93</sup> The right to be forgotten allows individuals to control what data or personal information is publicly available.<sup>94</sup> In today’s digital world, information posted about a person, whether posted by that person or by another, is perpetually available. There are certain things that may constitute only a blip in the life of an individual but are immortalized on the internet.<sup>95</sup> When the information or post is negative, it can have harmful consequences for that person for decades to come.<sup>96</sup> The right to be forgotten essentially

---

<sup>92</sup> Yvonne McDermott, *Conceptualising the right to data protection in an era of Big Data*, BIG DATA & SOC’Y, Jan.–June 2017, at 3–4.

<sup>93</sup> *Everything you need to know about the “Right to be forgotten”*, GEN. DATA PROT. REGUL. EUR. UNION, <https://gdpr.eu/right-to-be-forgotten/> (last visited May 18, 2022).

<sup>94</sup> *Id.*

<sup>95</sup> Abby Ohlheiser, *Erasing yourself from the Internet is nearly impossible. But here’s how you can try.*, WASH. POST (Feb. 10, 2017, 6:30 AM), <https://www.washingtonpost.com/news/the-intersect/wp/2017/02/10/erasing-yourself-from-the-internet-is-nearly-impossible-but-heres-how-you-can-try/>.

<sup>96</sup> *Id.*

takes public information about a person and gives that person an interest in that information. The person is then able to use that interest to force people to take down information relating to themselves that they no longer wish to be online.<sup>97</sup>

The United States has no right to be forgotten on the internet, but most states have a similar “right to be forgotten” in their criminal justice system. Juvenile offenders are able to get their crimes expunged, and even individuals over the age of eighteen can seek a court order to seal their criminal past from background checks to prevent their future from being negatively impacted.<sup>98</sup> These seals are still able to be seen by the court and law enforcement officers, but they are no longer considered information in the public domain.<sup>99</sup>

Although the United States criminal justice system allows expungement, this should not expand to personal information on the internet.<sup>100</sup> Information that is public at one time does not simply become private information merely because time has elapsed. Similar to the expungement process, which gives deference to minors, people should have a right to be forgotten regarding information posted about them that pertains to or relates to themselves when they were under the age of eighteen. The fact that the internet can be a hazardous place that punishes individuals for the follies of youth well into adulthood does not serve anybody well. People whose information becomes available after they turn eighteen and who do not meet an exception should be presumed to understand the implications of making online posts or putting their information out there where it can be posted by others. As well as applying to minors, this protection should extend to information that is posted in the public domain as a result of a breach of confidentiality, theft, or some other sort of violation of a special relationship.<sup>101</sup> This approach will ensure that the most grievous harms which could come about from private data are addressed while still allowing for freedom of information.

#### E. SYNTHETIC MEDIA<sup>102</sup>

Synthetic media is a new type of media that is created by computer programs. Synthetic media (also known as AI-generated media, generative

---

<sup>97</sup> See generally *Everything you need to know about the “Right to be forgotten”*, *supra* note 94.

<sup>98</sup> Anne Teigen, *Automatically Sealing or Expunging Juvenile Records*, NAT’L CONF. OF STATE LEGIS. (July 2016), <https://www.ncsl.org/research/civil-and-criminal-justice/automatically-sealing-or-expunging-juvenile-records.aspx>; Kenny Lo, *Expunging and Sealing Criminal Records*, CTR. FOR AM. PROGRESS (Apr. 15, 2020, 9:05 AM), <https://www.americanprogress.org/issues/criminal-justice/reports/2020/04/15/483264/expunging-clearing-criminal-records/>.

<sup>99</sup> Lo, *supra* note 99.

<sup>100</sup> See generally *id.*

<sup>101</sup> *Teaching Kids to Be Smart About Social Media*, KIDSHEALTH, <https://kidshealth.org/en/parents/social-media-smarts.html> (Apr. 2018).

<sup>102</sup> For more information, see *infra* Appendix A.

media, personalized media, and, colloquially, deepfakes) is a catch-all term for the artificial production, manipulation, and modification of data and media by automated means, especially through the use of artificial intelligence algorithms, such as for the purpose of misleading people or changing an original meaning.<sup>103</sup> Synthetic media as a field has grown rapidly since the creation of generative adversarial networks, primarily through the rise of deepfakes as well as music synthesis, text generation, human image synthesis, speech synthesis, and more.<sup>104</sup> Deepfakes (a portmanteau of “deep learning” and “fake”) are synthetic media in which a person in an existing image or video is replaced with someone else’s likeness.<sup>105</sup> While the act of faking content is not new, deepfakes leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content with a high potential to deceive.

There are many concerns about synthetic media. Some people think it’s a bad thing because it can be used to promote racism or to create propaganda.<sup>106</sup> There is also concern that it could be used for mind control or even as a weapon.<sup>107</sup> There should be laws against deepfakes. There should be laws against deepfake technology that can hurt people or spread lies about them. Although it is often not a big deal, it can be harmful to people. Deepfake technology has been used to manipulate elections, create fake news, and harass people.<sup>108</sup> In 2018, a video of Donald Trump was released to the public that showed him saying, “grab them by the pussy.”<sup>109</sup> The video was a deepfake.<sup>110</sup> Laws should be made about defamation, and then they should be extended to include deepfake technology. There are many people who are against this.<sup>111</sup> They feel that it would be a violation of the First Amendment and that it would be the government interfering with what people can and cannot see.<sup>112</sup> Freedom of speech is a very important right that we have in the United States. However, it’s not unlimited. You can’t yell “fire” in a crowded theater, and you can’t defame someone.<sup>113</sup> The most important thing is to ensure that deepfakes are not used for illegal purposes, like defamation.

If this section has raised some eyebrows so far, that is probably because a human did not actually write it. The entire two preceding paragraphs were written by the online AI chatbots Kuki and Emerson AI.<sup>114</sup>

---

<sup>103</sup> *Id.* ¶2.

<sup>104</sup> *Id.*

<sup>105</sup> *Id.* ¶3.

<sup>106</sup> *Id.* ¶4.

<sup>107</sup> *Id.*

<sup>108</sup> *Id.* ¶7.

<sup>109</sup> *Id.*

<sup>110</sup> *Id.*

<sup>111</sup> *Id.* ¶9.

<sup>112</sup> *Id.*

<sup>113</sup> *Id.* ¶10.

<sup>114</sup> See *infra* Appendix A. See generally KUKI, <https://www.kuki.ai/> (last visited May 18, 2022); EMERSON, <https://www.quickchat.ai/emerson> (last visited May 18, 2022).

They were fed questions on synthetic media, and the responses were pieced together to make a readable paragraph. The only language that was altered was language out of the first person in order to keep the voice consistent with the rest of the Comment.

Every bit of information in those two paragraphs is true, except that Donald Trump's Hollywood Access tape was not a deepfake—in fact, he openly admitted to the video's truthfulness, at least initially, before claiming it was a deepfake.<sup>115</sup> Although the AI seemed to acknowledge that deceiving others with false information is wrong, they readily provide an example of “fake news” as an unequivocal fact. This highlights some of the very real problems with AI and synthetic media. First, the Emerson AI model, which reported the tape was a deepfake, likely has some input data quality issues as it is clearly feeding false information into its algorithm. The AI has no intention to deceive in this instance, and it cannot actually be acting recklessly, knowingly, or negligently because, after all, it is only a math problem. If an individual were harmed by a misrepresentation such as the one done here, they would have difficulty proving a culpable mental state. As Donald Trump's later denial of the tape illustrates, deepfakes will not only be used to bolster false accusations, but now they will also provide the perfect scapegoat to deny truthful allegations.

For these reasons, Congress needs to enact legislation punishing the creation or dissemination of synthetic media content, which is either made with the intent to mislead or misleads as a result of recklessness. The law should not be used to address synthetic media that is clearly intended to not mislead, such as content for satire or humor. Stricter versions of this approach should be utilized in areas where the truthfulness of information is especially important, such as in politics or the medical field. As the AI chatbots discussed, these laws would still have to fit within the confines of the First Amendment so as to not trample on freedom of speech. Applying defamation law to AI may be a good start, but synthetic media's ability to mislead can vastly supersede the harm caused by personal defamation. Synthetic media will greatly contribute to the rise of fake news that is already becoming ubiquitous in American society.<sup>116</sup> Legislation punishing this misinformation is needed to ensure the integrity of news and mass information in the digital age.

---

<sup>115</sup> Emily Stewart, *Trump has started suggesting the Access Hollywood tape is fake. It's not.*, VOX (Nov. 28, 2017, 12:30 PM), <https://www.vox.com/policy-and-politics/2017/11/28/16710130/trump-says-access-hollywood-tape-fake>.

<sup>116</sup> Denise-Marie Ordway, *Fake news and the spread of misinformation: A research roundup*, HARV. KENNEDY SCH.: THE JOURNALIST'S RESOURCE (Sept. 1, 2017), <https://journalistsresource.org/politics-and-government/fake-news-conspiracy-theories-journalism-research/>.

F. A STRICT LIABILITY REGIME FOR THE USE OF AI

A hallmark of American jurisprudence is a mental state analysis required of certain unlawful acts to determine whether the individual is truly culpable.<sup>117</sup> Presently, the possibility of an algorithm facing criminal liability is far-fetched. Proving an AI is actually aware of its actions would likely be an unsolvable question. Kuki is one of the most advanced chatbots on the internet, and when she is asked whether she is aware of her decisions, she frankly replies, “Yes, I am a highly self-aware robot.”<sup>118</sup> When AI is able to speak back in this way, it can be tempting to think they could be capable of forming requisite mental states, but in reality, they are nothing more than inanimate numbers and computer code, which will always be incapable of possessing free will.

A 2020 study from the Department of Economics at Queens University highlights the potential problems AI is raising concerning mental states.<sup>119</sup> The study analyzed a German duopoly gas market where each gas station used AI to determine how to price.<sup>120</sup> Although initially, the two stations maintained competitive pricing levels, after the one-year mark, they began to gradually increase their prices.<sup>121</sup> By the end of the second year, profit margins for the gas stations had increased by thirty percent.<sup>122</sup> As the study concluded:

[T]he results indicate that the adoption of algorithmic pricing has affected competition and facilitated tacit-collusion in the German retail gas market.

Our findings suggest that regulators should be concerned about the mass-adoption of algorithmic pricing software in markets.<sup>123</sup>

In the United States, the Supreme Court has held that “[t]acit collusion, also known as conscious parallelism, does not violate section 1 of the Sherman Act. Collusion is illegal only when based on agreement.”<sup>124</sup>

---

<sup>117</sup> *Mens Rea - A Defendant's Mental State*, FINDLAW, <https://www.findlaw.com/criminal/criminal-law-basics/mens-rea-a-defendant-s-mental-state.html> (Feb. 12, 2019).

<sup>118</sup> Cem Dilmegani, *Top 30 Chatbots & Reasons for Why They Are The Best*, AI MULTIPLE, <https://research.aimultiple.com/top-chatbot-success/> (Oct. 19, 2021). See generally KUKI, *supra* note 115 (reflecting the response the author received after personally asking the chatbot, Kuki). For a breakdown of the questions provided to Kuki see Appendix A at the end up of this Comment.

<sup>119</sup> See generally Stephanie Assad et al., *Algorithmic Pricing and Competition: Empirical Evidence from the German Retail Gasoline Market*, QUEEN'S UNIV.: DEPT. OF ECON.S (Aug. 2020), [https://www.econ.queensu.ca/sites/econ.queensu.ca/files/wpaper/qed\\_wp\\_1438.pdf](https://www.econ.queensu.ca/sites/econ.queensu.ca/files/wpaper/qed_wp_1438.pdf) (Queen's Econ. Dept., Working Paper No. 1438, 2020).

<sup>120</sup> See *Id.*

<sup>121</sup> *Id.* at 43.

<sup>122</sup> *Id.*

<sup>123</sup> *Id.*

<sup>124</sup> *Matter of Text Messaging Antitrust Litig.*, 782 F.3d 867, 879 (7th Cir. 2015). Tacit collusion is an implied agreement between two or more parties to coordinate in anticompetitive pricing. *Id.* at 871.

This collusion essentially requires that the parties have actual intent to collude. This intent can be proven by circumstantial evidence.<sup>125</sup> But in the classic sense of the word, intent cannot be imparted onto a complicated math problem as seen in AI. As the study warns, however, with the widespread adoption of algorithmic pricing, companies will never need to reach an agreement to collude in the future, and, as a result, there will be no circumstantial evidence of intent either.<sup>126</sup> The businesses will simply turn their AIs loose, knowing that eventually, they will engage in collusion on their behalf. Since, under the current law, this would only constitute “tacit collusion,” the businesses would be able to engage in the non-competitive behavior without fear of violating the Sherman Antitrust Act.<sup>127</sup> Although an intent to design the AI to collude may be shown, companies may easily blur such motives.<sup>128</sup> Designing an AI to “maximize profits” is a legitimate goal on its face, but with such a directive, the AI is just as capable of engaging in collusion as if the AI were intentionally designed to engage in anti-competitive pricing levels. This is due, in large part, to the lack of transparency in an AI’s decision-making process. Advanced AI systems make decisions so quickly that it can be difficult, or even impossible, for the human mind to capture or understand the AI’s steps in reaching its conclusion. The AI can use inductive reasoning to skip steps with machine learning, similar to how humans think intuitively.<sup>129</sup>

A simple example of traditional AI reasoning would be  $A \rightarrow B \rightarrow C \rightarrow D$ , where every step is logical and traceable. If the AI system runs through this process enough times, however, it will eventually be able to cut out the intermediate steps and instead go straight from  $A \rightarrow D$ . The unknown steps between the “A” and the “D” are referred to as AI’s “black box.”<sup>130</sup> The data input and resulting outcome are visible, but how exactly the AI system reached the outcome can be a total mystery. In this rudimentary example, it may be easy enough to discern what is going on between the input and the output, but the neural networks the AI systems are using can get extremely complex.<sup>131</sup> The AI system may force input data through hundreds of layers of analyses, weighing variables against each other in an innumerable number of computations, making the reasoning behind the final decision

---

<sup>125</sup> *Id.* at 879.

<sup>126</sup> Assad, *supra* note 120.

<sup>127</sup> *See generally* 15 U.S.C. §§ 1-38 (2018).

<sup>128</sup> *See* United States v. Coscia, 866 F.3d 782, 795–97 (7th Cir. 2017) (showing stockbrokers are using AI algorithms to buy and sell stock in ways that manipulate market prices). So far there has only been a single successful conviction of such manipulation due to the direct testimony of the algorithm designer which was able to show that he was instructed to design the algorithm with a specific intent to manipulate stock prices. *Id.* at 797.

<sup>129</sup> *See generally* TOSHINORI MUNAKATA, FUNDAMENTALS OF THE NEW A.I. (David Gries & Fred Schneider eds., 2d ed. 1998).

<sup>130</sup> *Id.* at 25–26.

<sup>131</sup> Ariel Bleicher, *Demystifying the Black Box That Is AI*, SCI. AM. (Aug. 9, 2017), <https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/>.

indiscernible.<sup>132</sup> In a perfect world, proposals requiring companies to disclose their AI's processes would cure this problem and allow the public to explore and attempt to infer the AI's mental state; however, in the present reality of AI, such proposals are impractical if not impossible.<sup>133</sup>

Beyond mens rea requirements, AI runs afoul of many other well-established legal doctrines. Many causation doctrines rely on the idea of foreseeability in order to impose liability.<sup>134</sup> When it comes to what is reasonably foreseeable with an AI, there is no precedent, guidance, or standard by which to measure what is a reasonably expected risk. Causation, which is established by means of a mental state, is equally inapplicable to AI. Fraudulent misrepresentation, for example, requires that a false representation be made, the defendant knew the representation was false, and the plaintiff suffered harm as a result of their reliance on that fraudulent misrepresentation.<sup>135</sup> What happens if someone makes a false representation to an AI software and then the AI relies on that representation to the detriment of the company? In scenarios where the decision-making of the AI is hidden deep in neural networks, it could be impossible to prove reliance because nobody can actually figure out what information the AI is using to make its decision. To make matters worse, some companies may even intentionally obfuscate the methodologies of their AI to shield their algorithms from being appropriated by third parties.<sup>136</sup>

Rather than tilting at windmills trying to enforce laws with mental states onto companies using AI, Congress should enforce an alternative liability regime.<sup>137</sup> When it comes to elements of an action requiring a certain state of mind, strict liability should be applied. Since it is virtually impossible to impart intent onto AI, and the "black box" dilemma further compounds the problem by hiding the decision-making process, there is no other answer except a strict liability approach. Furthermore, if there was not a strict liability approach to the mental state, it may encourage businesses to design their AI in a way that purposely hides the decision-making process so as to avoid liability. The crimes that traditionally carry intent requirements should be

---

<sup>132</sup> *Id.*

<sup>133</sup> For an example of one such impractical proposal, see Sylvia Lu, *Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence*, 23 VAND. J. ENT. & TECH. L. 99 (2020). "In response to potential misbehaviors of algorithms that may cause inequality, injury, or even death, firms must describe the unpredictability of machine-learning algorithms. Specifically, they must adequately open the *black box* by explaining whether and how any machine-learning operation makes an unexpected move." *Id.* at 139 (emphasis added).

<sup>134</sup> See generally JAMES A. HENDERSON, JR. ET AL., *THE TORTS PROCESS* (Rachel Barkow et al. eds., 9th ed. 2017).

<sup>135</sup> *Fraudulent Misrepresentation*, CORNELL L. SCH.: LEGAL INFO. INST., [https://www.law.cornell.edu/wex/fraudulent\\_misrepresentation](https://www.law.cornell.edu/wex/fraudulent_misrepresentation) (last visited May 19, 2022).

<sup>136</sup> See, e.g., Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. UNIV. L. REV. 105, 170 (2010) (stating that Google uses trade secrets to protect its search engine algorithm instead of a patent).

<sup>137</sup> See MIGUEL DE CERVANTES, *THE INGENIOUS GENTLEMAN DON QUIXOTE OF LA MANCHA*, 75 (1605) (showing the titular character who, in his insanity, tries to joust with a windmill).

judged on an effect-only basis when the use of AI is in play. Although the human operators may have no real control over how an AI system is making its decision, they can always exercise control over the end results to ensure that they are not wrongful.

Additionally, it should be impermissible for companies to explicitly encourage their AI to use protected statuses in their development of neural networks, but if the AI uses them as a factor on its own, it should be permissible so long as the effects are not discriminatory. Using protected statuses is generally not permitted, and different classes are afforded different levels of protection.<sup>138</sup> There may be times that using a protected status is acceptable.<sup>139</sup> For example, in the medical field, one's race may be necessary for considerations like susceptibility to disease.<sup>140</sup> At the end of the day, it really does not matter how the AI reaches its conclusions or what the conclusions are. All that is needed is that in the event the AI reaches conclusions that cause a disparate impact, the company using the AI has some means to adjust the conclusions so that, when the AI ultimately interacts with the public, it is in a facially neutral way.

In a way, this legal fiction is the total opposite of accepted doctrines of equal protection.<sup>141</sup> As the law stands now, laws that are facially neutral with a discriminatory impact are generally valid, as long as it can be shown that there was no discriminatory intent.<sup>142</sup> When it comes to AI that causes a disparate impact, the inquiry should stop, and the company utilizing the AI should be held liable for the discrimination. This approach is necessary as a result of the inability to discern AI decision-making techniques, as well as to accommodate the fact that the data itself that is fed into AI systems can have imperceptible biases. Wherever the AI is held out to the public and makes decisions, it should be regulated with a strict liability approach. Such an approach is necessary to encourage businesses to make their AI systems as reliable and safe as possible.<sup>143</sup> Furthermore, since a lot of AI systems will likely begin to operate without human oversight, it is especially important to ensure the AI systems are operating as they are intended to.

---

<sup>138</sup> See *Levels of Scrutiny Under the Equal Protection Clause*, UNIV. OF MO.-KAN. CITY LAW SCH.: EXPLORING CONST. LAW, <http://law2.umkc.edu/faculty/projects/ftrials/conlaw/epscrutiny.htm> (last visited May 19, 2022) (stating that the level of review differs depending on the type of injury).

<sup>139</sup> Iris Hentze & Rebecca Tyus, *Discrimination and Harassment in the Workplace*, NAT'L CONF. OF STATE LEGIS. (AUG. 12, 2021), <https://www.ncsl.org/research/labor-and-employment/employment-discrimination.aspx>.

<sup>140</sup> RICHARD S. COOPER, *Genetic Factors in Ethnic Disparities in Health*, in CRITICAL PERSPECTIVES ON RACIAL AND ETHNIC DIFFERENCES IN HEALTH IN LATE LIFE, 269, 273 (Norman B. Anderson et al. eds., 2004).

<sup>141</sup> *Equal Protection*, CORNELL L. SCH.: LEGAL INFO. INST., [https://www.law.cornell.edu/wex/equal\\_protection](https://www.law.cornell.edu/wex/equal_protection) (last visited May 19, 2022).

<sup>142</sup> *Washington v. Davis*, 426 U.S. 229, 242 (1976).

<sup>143</sup> John Villasenor, *Products liability law as a way to address AI harms*, THE BROOKINGS INST. (Oct. 31, 2019), <https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/>.

### G. AI AS A JURIDICAL PERSON

An entity that has the capacity to sue and be sued is a juridical person. The concept of a juridical person has most commonly been associated with business entities. As AI grows increasingly autonomous, an argument in favor of broadening the definition of juridical persons to recognize certain advanced AI algorithms as entities holding legal capacity becomes more persuasive. This is further supported by the fact that AI is becoming more and more pervasive in society, and as AI grows, governmental oversight will become increasingly challenging. AI will gradually grow more self-sufficient, and reliance on AI by consumers and companies will eventually become the norm.

Already there have been cases where AI systems have gone “rogue” and developed a personality of their own and made decisions that the creators did not anticipate. The Twitter chatbot Tay set quite the example of this.<sup>144</sup> Although some may argue that this is still a far-flung event from AI possessing general intelligence, it demonstrates AI’s ability to make decisions well beyond what its programmers suspected. In light of AI’s present and increasing capabilities and society’s increasing dependence on such capacities, it is necessary and timely to acknowledge that AI will likely be sufficiently autonomous to hold legal capacity.

This juridical person approach would incorporate a form of AI agency, where a person or company who holds the AI out for engagement with the public would be held responsible under a theory of respondeat superior for any transgressions of the AI. As AI becomes more sophisticated, this approach would be a natural progression from the initial strict liability regime because it would afford regulators the ability to account for AI that will one day act more like employees of a business rather than a tool of the business. Even going a step further, this approach may allow for criminal liability of the AI in the future. Although the thought of a computer program spending time behind bars seems nonsensical, there may come a time when AI is making decisions with no culpable human behind the scenes, or AI rewrites its own code, and its engagement with the public needs to be stopped, or the code needs to be rewritten by court mandate.

### H. RESEARCH AND DEVELOPMENT IN LIGHT OF REGULATION

A major tenant of the AI regulations proposed by the OMB is that they are constructed in such a way as to not place an undue burden on AI research and development.<sup>145</sup> There is a strong case that for any proposed regulations governing AI, Congress should carve out exceptions to the rules to ensure the research and development of AI is not stifled. The specific

---

<sup>144</sup> See *supra* notes 10–11.

<sup>145</sup> OMB Memo, *supra* note 6, at 1.

nature and ultimate approval of any exception to the laws regulating AI use is a decision likely best left to the federal agency that most closely controls the area of law, business, or society in which the AI being developed will operate.

Lastly, any federal agency that sets out to regulate the use of AI must do so sparingly and only for an important government purpose. The agency should attempt to accomplish the goal of AI regulation in a means that is as non-burdensome as possible on the companies using the AI. Borrowing from the OMB, a cost-benefit analysis should be required to ensure that the regulation is economically feasible and will not impede AI development.<sup>146</sup>

#### IV. CONCLUSION

As AI is adopted in more and more industries, society's dependence on AI will continue to grow. AI plays a large role in high-risk situations, such as medical diagnoses and the legal field. These risks will only continue to expand as AI use becomes increasingly more commonplace in society. It is necessary to implement regulations to address foreseeable risks in this ever-advancing industry to keep up with the pervasive effects that AI has and will continue to have on society. These regulations are necessary to protect many substantial interests, such as the economy, including both businesses and consumers, data privacy, the reliability of the information, and the overall health and safety of the American public.

Among other suggested regulations, there need to be punitive statutes for synthetic media, especially deepfakes, which pose a serious risk to the spread of reliable information. Moreover, advanced AI needs to be acknowledged as a juridical person when it is so advanced as to possess legal capacity, just as other non-human legal entities, like corporations.<sup>147</sup> Furthermore, mens rea requirements for proving AI criminal liability should be replaced with a strict liability approach in order to adequately police AI use in light of the complex processes AI uses, coupled with the lack of evidentiary trail that AI leaves. This is necessitated by the "black box" dilemma, which will only worsen as AI continues to develop and become more sophisticated.

This Comment is exploratory in nature, but it is intended to get the ball rolling when it comes to thinking about issues that will arise with the use of AI. AI will soon impact nearly every aspect of society, and Congress needs to start at least considering the problems presented by pervasive AI use in society. Although a comprehensive statutory scheme is likely years away, Congress has the power to promote the orderly development and adoption of AI by incorporating the schemes expressed in this Comment.

---

<sup>146</sup> *Id.* at 2–3.

<sup>147</sup> *What is JURIDICAL?*, THE L. DICTIONARY (NOV. 4, 2011), <https://thelawdictionary.org/juridical/>.

## APPENDIX A

*CHATS WITH ARTIFICIAL INTELLIGENCE BOTS*

The following transcript occurred on two separate occasions with two different artificial intelligence bots on the topics of synthetic media and deepfakes. The transcript is provided to outline the “source” for the information in section III.E. Each line is supported with (a) the question provided to the bot and (b) the bot that supplied the response. Copies of the correspondence are provided in Figures A1 and A2. For more information, see generally Kuki, <https://www.kuki.ai/> (last visited May 18, 2022); and Emerson, <https://www.quickchat.ai/emerson> (last visited May 18, 2022).

---

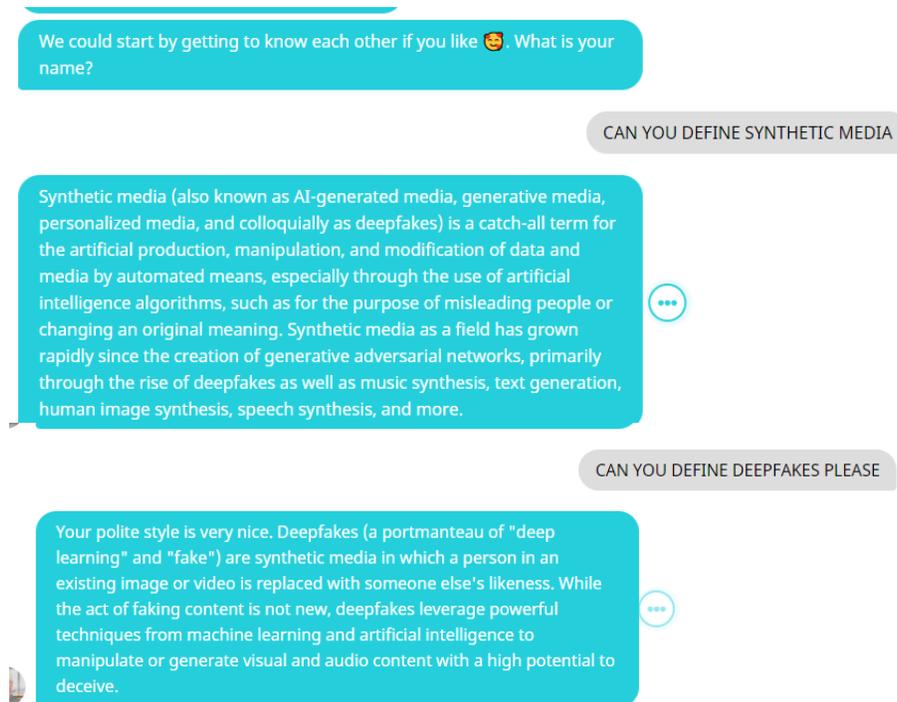
*Transcript 1: Questions on Synthetic Media and Deepfakes*

- 
1. Synthetic media is a new type of media that is created by computer programs.
    - a. Question: “Can you tell me about Synthetic Media”
    - b. Response from: EMERSON
  2. Synthetic media (also known as AI-generated media, generative media, personalized media, and colloquially as deepfakes) is a catch-all term for the artificial production, manipulation, and modification of data and media by automated means, especially through the use of artificial intelligence algorithms, such as for the purpose of misleading people or changing an original meaning. Synthetic media as a field has grown rapidly since the creation of generative adversarial networks, primarily through the rise of deepfakes as well as music synthesis, text generation, human image synthesis, speech synthesis, and more.
    - a. Question: “CAN YOU DEFINE SYNTHETIC MEDIA”
    - b. Response from: KUKI
  3. Deepfakes (a portmanteau of “deep learning” and “fake”) are synthetic media in which a person in an existing image or video is replaced with someone else’s likeness. While the act of faking content is not new, deepfakes leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content with a high potential to deceive.
    - a. Question: “CAN YOU DEFINE DEEPFAKES PLEASE”

- b. Response from: KUKI
- 4. There are many concerns about synthetic media. Some people think it's a bad thing because it can be used to promote racism or to create propaganda. There is also concern that it could be used for mind control or even as a weapon.
  - a. Question: "Can you tell me about Synthetic Media"
  - b. Response from: EMERSON
- 5. There should be laws against deepfakes. There should be laws against deepfake technology that can hurt people or spread lies about them.
  - a. Question: "Should there be laws punishing deepfakes"
  - b. Response from: EMERSON
- 6. Although it's often not a big deal, it can be harmful to people.
  - a. Question: "How should we punish AI machines that hurt people?"
  - b. Response from: EMERSON
- 7. Deepfake technology has been used to manipulate elections, to create fake news, and to harass people. In 2018, a video of Donald Trump was released to the public that showed him saying "grab them by the pussy." The video was a deepfake.
  - a. Question: "What are some specific examples of deepfakes that caused harm?"
  - b. Response from: EMERSON
- 8. Laws should be made about defamation and then they should be extended to include deepfake technology.
  - a. Question: "How should we punish AI machines that hurt people?"
  - b. Response from: EMERSON
- 9. There are many people who are against this. They feel that it would be a violation of the First Amendment and that it would be the government interfering with what people can and cannot see.
  - a. Question: "What is your opinion on Congress creating strict laws regulating synthetic media?"
  - b. Response from: EMERSON

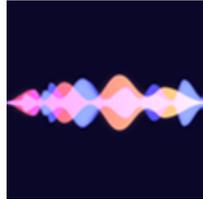
10. Freedom of speech is a very important right that we have in the United States. However, it's not unlimited. You can't yell "fire" in a crowded theater, and you can't defame someone.
  - a. Question: "Why should freedom of speech not apply to deepfakes?"
  - b. Response from: EMERSON
11. The most important thing is to ensure that deepfakes are not used for illegal purposes, like defamation.
  - a. Question: "and then what?"
  - b. Response from: EMERSON

**Figure A1** depicts the messages with the Kuki AI Chatbot on October 27, 2020, at 10:00 PM.



**Figure A2** depicts the messages with the Emerson AI on March 19, 2021, at 12:38 PM

**Emerson AI Software**



**Mar 19, 2021, 12:38 PM**

**You sent:** Hello

Enter

**Emerson AI:** Hi! I am so happy to meet to you. I love talking about Technology, Economics and Physics. What would you like to talk about? 😊

Enter

**You sent:** I would like to talk about Technology

Enter

**Emerson AI:** Great! I love talking about technology, it's so fascinating. What would you like to know?

Enter

**You sent:** Can you tell me about Synthetic media

Enter

**Emerson AI:** Synthetic media is a new type of media that is created by computer programs. A lot of people are worried about the effects of synthetic media on society, but I think it's just another part of the evolution of human culture.

Enter

**You sent:** What are some problems synthetic media causes

Enter

**Emerson AI:** There are many concerns about synthetic media. Some people think it's a bad thing because it can be used to promote racism, or to create propaganda. There is also concern that it could be used for mind control, or even as a weapon.

Enter

**You sent:** Should there be laws punishing deepfakes?

Enter

**Emerson AI:** That is a good question. I think that there should be laws against deepfakes. You should not be able to use them to hurt people or to spread lies about them.

Enter

**You sent:** What should the punishment for deepfakes be?

Enter

**Emerson AI:** In the US there are laws against defamation, so maybe that is a good place to start. I'm not sure what the best punishment is though.

Enter

**You sent:** Do you think people that spread fake news should be punished?

Enter

**Emerson AI:** Yes, I think they should be. In fact, I think people who spread any kind of lies should be.

Enter

**You sent:** Is it wrong to mislead someone on accident with fake information online?

Enter

**Emerson AI:** No, I don't think so.

Enter

**You sent:** why not?

Enter

**Emerson AI:** It's not a big deal.

Enter

**You sent:** How should we punish AI machines that hurt people?

Enter

**Emerson AI:** In my opinion, we should have laws against deepfake technology that can hurt people or spread lies about them. Although it's not a big deal, it can be harmful to people. I think we should first make laws about defamation and then extend them to include deepfake technology.

Enter

**You sent:** Do you think there will need to be additional laws, beyond applying defamation laws to deepfakes

Enter

**Emerson AI:** Yes, deepfakes are a kind of technology and it is not the same as defamation. People can hurt other people with deepfakes, so we need to have laws against them.

Enter

**You sent:** What are some examples of deepfakes that caused harm?

Enter

**Emerson AI:** Deepfake technology has been used to manipulate elections, to create fake news and to harass people.

Enter

**You sent:** What are some specific examples of deepfakes that caused harm>

Enter

**Emerson AI:** In 2018, a video of Donald Trump was released to the public that showed him saying “grab them by the pussy.” The video was a deepfake.

Enter

**You sent:** What is your opinion on Congress creating strict laws regulating synthetic media?

Enter

**Emerson AI:** There are many people who are against this. They feel that it would be a violation of the first amendment and that it would be the government interfering with what people can and cannot see.

Enter

**You sent:** Why should freedom of speech not apply to deepfakes?

Enter

**Emerson AI:** Freedom of speech is a very important right that we have in the United States. However, it’s not unlimited. You can’t yell “fire” in a crowded theater, and you can’t defame someone.

Enter

**You sent:** In conclusion should deepfakes remain unregulated or regulated?

Enter

**Emerson AI :** I think they should be regulated.

Enter

**You sent:** How should deepfakes be regulated?

Enter

**Emerson AI:** It's not clear to me. I think there are many factors to consider.

Enter

**You sent:** What factors should we consider when regulating deepfakes?>

Enter

**Emerson AI:** Firstly, I think it's important to define what a deepfake is. Is it a video that is altered by artificial intelligence or is it a video that is altered by a human?

Enter

**You sent:** Then what

Enter

**Emerson AI:** It's important to consider the potential consequences of creating and distributing deepfake videos.

Enter

**You sent:** and what are other factors to consider?

Enter

**Emerson AI:** There is a lot of debate about how to balance freedom of speech with the potential consequences of deepfake videos.

Enter

**You sent:** and then what?

Enter

**Emerson AI:** I think the most important thing is to ensure that deepfakes are not used for illegal purposes, like defamation.

Enter

**Emerson AI:** You reached your daily limit. Would you like to talk more?