Zenarosa, Jason

Prof. Bell

WR60 Sec. 33306

25 February 2023

Balancing Innovation and Accountability: The Need for Stricter Regulation of AI

Artificial Intelligence (AI) has rapidly emerged as a technology that is shaping and transforming various aspects of our lives. AI has the potential to bring unprecedented benefits to society, and it continues to be integrated in almost every industry. However, as AI becomes more widespread, concerns have also emerged about its potential negative impact. For example, it can be used to spread disinformation or impersonate people without their consent through the use of deepfakes. Additionally, the use of AI by government bodies such as the police and border control disproportionately affects marginalized groups such as people of color and undocumented immigrants (Read this to find out more about how the use of AI can potentially be harmful). The purpose of this essay is to argue that there is a lack of regulation for AI technology in the US and to propose solutions to this issue. Although it could be argued that creating legislation with the purpose of regulating AI will only serve to hinder the advancement and innovation of this emerging technology, the criminalization of certain use cases of AI would help to keep the American public safe. These use cases include the police and border control's use of biometric recognition technology, as well as the use of deepfakes to impersonate or even create pornography of people without their consent.

As AI technology rapidly develops, there is increased pressure on governmental agencies to create legislation with the purpose of protecting people from the potential harms associated with AI. This has led to some efforts by the federal government to rectify this issue, such as the

National AI Initiative and the Blueprint for an AI Bill of Rights. However, these existing solutions are insufficient, as they do not criminalize malicious misuse of AI.

According to their official website, the National AI Initiative is a US government-led effort established by the National Artificial Intelligence Initiative Act of 2020 to ensure continued US leadership in AI R&D, lead the world in the development of trustworthy AI systems, prepare the present and future workforce for AI integration across all sectors of the economy, and coordinate ongoing AI activities across all Federal agencies (National AI Initiative).

- **Innovation**
- **Advancing Trustworthy AI**
- **Education and Training**
- **Infrastructure**
- **Applications**
- **International Cooperation**

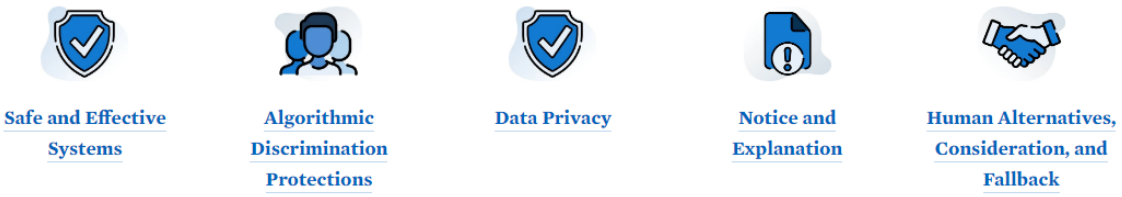
The emblem and Six Strategic Pillars of the National AI Initiative (National AI Initiative).

Out of the pillars listed above, the one most focused on upholding the safety and security of the American public is **Advancing Trustworthy AI**. Based on this pillar, several sectors of government, including the Food and Drug Administration, Federal Trade Commission, Consumer Product Safety Commission, and Equal Employment Opportunity Commission have issued guidelines on safe and ethical AI usage (National AI Initiative). For instance, pictured to

Good Machine Learning Practice for Medical Device Development: Guiding Principles	
Multi-Disciplinary Expertise Is Leveraged Throughout the Total Product Life Cycle	Good Software Engineering and Security Practices Are Implemented
Clinical Study Participants and Data Sets Are Representative of the Intended Patient Population	Training Data Sets Are Independent of Test Sets
Selected Reference Datasets Are Based Upon Best Available Methods	Model Design Is Tailored to the Available Data and Reflects the Intended Use of the Device
Focus Is Placed on the Performance of the Human-AI Team	Testing Demonstrates Device Performance During Clinically Relevant Conditions
Users Are Provided Clear, Essential Information	Deployed Models Are Monitored for Performance and Re-training Risks are Managed

the right are the guidelines set out by the FDA regarding AI and machine learning (FDA 1). These guidelines are useful resources for companies and organizations that want to start using and developing AI technology. However, they are generally very vague, and they don't actually take action against harmful or malicious misuse of AI. Overall, the National AI Initiative is a step in the right direction, it doesn't actually do anything to ensure that AI cannot be misused against people.

The Blueprint for an AI Bill of Rights is a document published by the White House in October 2022, outlining the federal government's guidelines for creating AI system's with the safety of the American public in mind.



The Five Principles of the Blueprint for an AI Bill of Rights (The White House).

According to the White House's official website, the Blueprint serves as "a handbook for anyone seeking to incorporate these protections into policy and practice" (The White House). The Blueprints principles encourage those developing AI to focus on the privacy of individuals, be transparent about how they are using AI, and make efforts to prevent discrimination. However, similarly to the FDA guidelines discussed previously, it does nothing to prevent the misuse of AI

by the police, the porn industry, or those looking to spread disinformation. Again, while the Blueprint is a step in the right direction, it doesn't actually propose any specific solutions to the issues currently being caused by AI.

By comparison, other countries have slightly more developed legislation than the US when it comes to AI regulation. For example, according to Chanley T. Howell, an intellectual property lawyer specializing in "Data Privacy and Security Compliance," China passed a regulation in March 2022 governing the use of algorithms in online recommendation systems (Howell). The regulation requires companies to notify users when an AI algorithm is being used to determine displayed information and provide users the option to opt out (Howell). The regulation also prohibits the use of personal data by algorithms to offer different prices to consumers (Howell). This regulation prevents consumers from being manipulated by companies through the use of AI by setting strict boundaries that companies must comply with in order to avoid legal action.

Additionally, according to Rita Liao, a tech journalist based in Asia, "The Cyberspace Administration of China… recently passed a regulation on 'deep synthesis' technology," which will force providers of AI-generative services (such as companies developing deepfakes and AI art) to "audit AI-generated content and user prompts manually or through technical means" (Liao). In other words, AI synthesizer companies must keep track of who is using their products. In addition, people who utilize AI-synthesized content will be held legally accountable if that content is used to "generate and disseminate fake news" (Liao). This is an incredible step for China against the abuse of deepfake technology.

That being said, China's regulations are by no means comprehensive; for example, it does nothing to prevent the misuse of AI by government bodies themselves. However, compare these

regulations to the weak and flimsy guidelines laid out by government bodies in the US, and it becomes clear that the US is lacking sufficient federal AI legislation.

So, what should be done? In order to decide what kind of legislation should be made, let's take another look at the key issues that are currently being caused by AI. The use of biometric recognition technologies in law enforcement and border control can exacerbate existing systemic biases and discrimination, leading to the unjust targeting of marginalized communities. Studies have shown that these technologies are more likely to misidentify people with darker skin tones, which means that they disproportionately harm Black, Indigenous, and People of Color (BIPOC) communities. This can lead to unfair and potentially harmful outcomes, such as false arrests, detention, and harassment. Therefore, certain government bodies, such as the police and border control, should be legally restricted from using AI biometric recognition. American policymakers must create legislation which criminalizes the act of arresting or detaining people simply based on AI biometric recognition. This will restrict law enforcement from abusing AI technology ensuring that government bodies are held accountable for their actions and that marginalized communities are not unfairly targeted or discriminated against.

Additionally, following suit with China, American policymakers should make legislation regulating companies that offer AI-generative services. Companies should keep track of the content that their software is being used to generate as well as who is using their software. In addition, things like spreading disinformation using AI-generated content and creating deepfake pornography without consent of those being impersonated should be criminalized. These policies will help keep individuals accountable for the way that they use AI and prevent it from being used with malicious intent.

Some argue that the regulation of AI technology may hinder its development and innovation. As a rapidly evolving field, AI technology requires flexibility and room for experimentation to reach its full potential. Excessive regulation could restrict research and development and reduce investment in the field. Furthermore, regulation could lead to a fragmented global market, with countries implementing different rules and standards, making it difficult for companies to operate and innovate globally. Additionally, some argue that AI regulation will be too difficult to implement effectively. Dr. Matt O'Shaughnessy, a visiting fellow at the Carnegie Endowment for International Peace with a PhD in Electrical and Computer, one issue with AI regulation is simply defining what AI is:

> *"Subtle differences in definition—as well as the overlapping and loaded terminology different actors use to describe similar techniques—can have major impacts on some of the most important problems facing policymakers"*
>
> - Dr. Matt O'Shaughnessy

However, while regulation may be difficult to implement and potentially hinder the development and innovation of AI technology, it is necessary to ensure that it is developed and used in a safe and ethical manner. Additionally, the legislation proposed above only restricts certain aspects of AI, which will not be too detrimental to its development. Unregulated AI technology can pose significant risks to the safety and wellbeing of individuals and our society as a whole. As such, regulation is necessary to ensure that AI is integrated safely into our society.

In conclusion, the regulation of AI is a necessary step towards ensuring that this powerful technology is used ethically and for the greater good. While some argue that regulation will stifle innovation, it is important to acknowledge the potential harms that unregulated AI can cause,

such as perpetuating societal biases, spreading disinformation, and facilitating identity theft. The current legislative landscape varies widely between different countries and the effectiveness of existing regulation is questionable. The proposed solutions, such as the White House's Blueprint for an AI Bill of Rights, provide useful guidelines but lack specific measures for enforcement. To be effective, AI regulation should include measures such as outlawing deepfakes without consent and restricting the use of biometric recognition software by the police and border control. While it is true that regulation may slow down innovation, it is important to remember that the potential risks of unregulated AI far outweigh any temporary delays in technological advancement. Ultimately, striking a balance between innovation and accountability is necessary to ensure that AI serves humanity in the safest and most effective way.

Works Cited

"Advancing Trustworthy Ai." *National Artificial Intelligence Initiative*, National Artificial Intelligence Initiative, 8 Feb. 2023, https://www.ai.gov/strategic-pillars/advancing-trustworthy-ai/.

"Blueprint for an AI Bill of Rights." *The White House*, The United States Government, 4 Oct. 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

Engler, Alex. "The EU and U.S. Are Starting to Align on AI Regulation." *Brookings*, Brookings, 9 Mar. 2022, https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation/.

Felz, Daniel J, et al. "AI Regulation in the U.S.: What's Coming, and What Companies Need to Do in 2023: News & Insights: Alston & Bird." *AI Regulation in the U.S.: What's Coming, and What Companies Need to Do in 2023 | News & Insights | Alston & Bird*, Alston & Bird, 9 Dec. 2022, https://www.alston.com/en/insights/publications/2022/12/ai-regulation-in-the-us#:~:text=This%20past%20year%20saw%20initial,AI%20in%20the%20United%20States.

Gold, Ashley. "AI Rockets Ahead in Vacuum of U.S. Regulation." *Axios*, Axios, 30 Jan. 2023, https://www.axios.com/2023/01/30/ai-chatgpt-regulation-laws.

"Good Machine Learning Practice for Medical Device Development: Guiding ..." *The Food and Drug Administration*, The Food and Drug Administration, https://www.fda.gov/media/153486/download.

Howell, Chanley T. “Ai Regulation: Where Do China, the EU, and the U.S. Stand Today?” *The National Law Review*, Foley & Lardner, 3 Aug. 2022, https://www.natlawreview.com/article/ai-regulation-where-do-china-eu-and-us-stand-today.

Lehot, Louis. *Artificial Intelligence Comparative Guide - - United States*, Foley & Lardner, 6 Dec. 2022, https://www.mondaq.com/unitedstates/technology/1059776/artificial-intelligence-comparative-guide.

Liao, Rita. “China's Generative AI Rules Set Boundaries and Punishments for Misuse.” *TechCrunch*, TechCrunch, 13 Dec. 2022, https://techcrunch.com/2022/12/13/chinas-generative-ai-rules-set-boundaries-and-punishments-for-misuse/.

O'Shaughnessy, Matt. “One of the Biggest Problems in Regulating AI Is Agreeing on a ...” *The Carnegie Endowment for International Peace*, The Carnegie Endowment for International Peace, 6 Oct. 2022, https://carnegieendowment.org/2022/10/06/one-of-biggest-problems-in-regulating-ai-is-agreeing-on-definition-pub-88100.

“Strategic Pillars.” *National Artificial Intelligence Initiative*, National Artificial Intelligence Initiative, 24 Apr. 2021, https://www.ai.gov/strategic-pillars/.