

Artificial Intelligence (AI) Safe Development, Deployment and Regulation Act

(DRAFT May 3, 2023)

The purpose is to regulate the safe development, and deployment of artificial intelligence (AI) to ensure alignment with the values of human dignity, autonomy, national security, personal privacy, national sovereignty, and safety, to promote responsible and ethical research, development, and use of AI and to protect the American people from foreign born AI-driven psychological influence.

Section 1: Definitions

"Artificial Intelligence" refers to computer systems that can perform tasks that would normally require human intelligence, including but not limited to machine learning, deep learning, natural language processing, and computer vision.

"AI system" refers to any artificial intelligence technology that is designed, developed, or deployed for a specific purpose.

"AI-driven psychological programming" refers to the use of artificial intelligence (AI) techniques and algorithms to influence emotions, attitudes, beliefs, or behaviors of an individual or group. This involves the use of large amounts of data, such as personal information, geotracking and online activities, to develop a profile of the individual or group and then using this profile to tailor and deliver targeted messaging or interventions. AI-driven psychological programming can be used in a manipulative or unethical manner, particularly if the individual is not aware that they are being influenced or if the programming is being used to spread selective, false or misleading information.

"Asilomar AI Principles" refers to a set of guidelines developed by a group of AI researchers, ethicists, and experts to promote the ethical and responsible development and safe deployment of artificial intelligence (AI) systems. Some key principles include the need for transparency, explainability, fairness, privacy and accountability in AI systems that does not exclude social and economic impacts. They aim to ensure that AI systems are developed in a way that aligns with human values, promotes human well-being, and respects human rights.

"Harm" refers to any injury or damage that results from a wrongful act or omission. In the context of consumer protection and unfair or deceptive practices, harm refers to any type of harm that a consumer may experience because of a company's actions, including financial harm,

physical harm, emotional harm, or reputational harm. Harm may include intangible harm, such as loss of privacy or loss of trust.

Section 2: Principles of Safe Development and Regulations

The development and deployment of AI systems must be guided by the principles of transparency, explainability, fairness, privacy, and accountability as outlined in the Asilomar AI Principles. This means that AI systems must be developed in a way that is open and transparent, and the decision-making processes of AI systems must be explainable to ensure that they do not operate in a way that is discriminatory, biased or a threat to national security. Furthermore, AI systems must be developed with respect for personal privacy, national security and AI developers must be held accountable for the decisions made by their systems.

AI systems must be developed in a way that respects individual dignity and promotes autonomy, and AI systems must not be developed in a way that could harm individuals or groups. AI systems must be developed in a way that ensures that humans remain in control of decision-making processes, and that decisions made by AI systems are subject to human review, intervention and stoppage when deemed manipulative in ways that degrade our national defense, the sovereignty of our country and the personal sovereignty of each American citizen. It is important to ensure that any use of AI-driven psychological programming is done in an ethical and transparent manner, with clear informed consent and protections for individuals' privacy and autonomy.

Section 3: Regulation of Safe AI Development and Deployment

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST works to develop and maintain a wide range of measurement standards and technologies, including those related to computing, communications, manufacturing, and cybersecurity. This includes establishing best practices and standards for the development and deployment of artificial intelligence (AI) systems, which is a growing area of focus for NIST. NIST also provides guidance to industry and government agencies on how to implement these standards in their own AI systems. NIST plays a critical role in advancing technological innovation and ensuring that emerging technologies are developed and deployed in a way that is safe, reliable, and aligned with societal values.

NIST shall establish standards for the development and deployment of AI systems to ensure that they are transparent, explainable, fair, private, accountable and prevent foreign AI-driven psychological programming of American citizens. NIST will coauthor these standards with all applicable federal agencies. These standards will provide guidance to AI developers and deployers on best practices for developing AI systems that align with the Asilomar AI Principles.

NIST shall work in collaboration with other federal agencies, industry experts, and civil society to establish and maintain these standards.

The Department of Commerce shall establish a certification program for AI systems that meet the standards established by NIST. This certification program will allow consumers and businesses to identify AI systems that have been developed in a responsible and ethical manner. The Department of Commerce shall also establish a process for revoking certification for AI systems that violate the standards established by NIST.

Section 4: Oversight and Accountability

In U.S. born companies, the Federal Trade Commission (FTC) shall have the authority to investigate and enforce compliance with this Act and may impose civil penalties for violations of the standards established by NIST. No AI developer or deployer may legally use an AI system that does not possess NIST certification and doing so will be deemed a violation of the Federal Trade Commission Act and may result in criminal prosecution by the Department of Justice. This includes the use of AI systems to spread disinformation, misinformation, interfere with elections, and incite violence or hatred against individuals or groups within the United States. The Department of Justice shall work in collaboration with other federal agencies to establish guidelines for identifying and prosecuting organizations, and individuals that violate this prohibition.

This will ensure that AI developers and deployers are held accountable for developing AI systems that do not align with the Asilomar AI Principles. The FTC shall work in collaboration with NIST and other federal agencies to enforce compliance with the standards established under this Act. In non-U.S. born companies all AI systems deemed a threat to national security shall be turned over to the Department of Justice, the Department of Homeland Security and when deemed part of a military operation, the Department of Defense. When the FTC has jurisdiction over foreign businesses, the FTC shall take legal action against developers and deployers of AI systems, seeking injunctive relief, consumer redress, and other remedies. The FTC may work with international law enforcement agencies and regulators to investigate and prosecute cross-border scams and other violations of consumer protection laws. The FTC may work with established partnerships from several international organizations, including the International Consumer Protection and Enforcement Network (ICPEN), to share information and coordinate enforcement efforts.

Individuals who are harmed by AI systems that violate the standards established by NIST shall have the right to seek criminal and civil legal remedies. This includes the right to sue AI developers and deployers for damages resulting from the use of AI systems that violate the standards established by NIST. Harm may constitute nothing more than the collection of personal data for the use of foreign AI driven psychological programming by current and emergent methods. The standard for “harm” will remain at the lowest possible criteria since the use of such data is often clandestine and true impact cannot be assessed by the average American without access to intelligence sources and methods. Causing such harm may constitute criminal

prosecution of AI developers and deployers who intentionally cause such acts in accordance with local, state and federal laws aimed to protect persons who have been harmed.

The Secretary of Commerce shall report annually to Congress on the implementation of this Act, including a description of any violations and enforcement actions taken, and other agencies involved as well as any updates to the standards established by NIST. Any updates by NIST must be done with the agencies who originally coauthored the original standards.

Section 5: Funding

There is authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act. Funds appropriated under this section shall be used for research, development, implementation and enforcement of the standards established by NIST, as well as for programs to promote responsible and ethical development of AI as set forth by NIST with their coauthors.

Section 6: Severability

If a court or legal authority finds that a particular provision of the Act is invalid or unconstitutional, it does not automatically invalidate the entire Act or other provisions within it. Instead, the rest of the Act remains in effect, and the provision in question will only be invalidated for that particular person or circumstance. This Act is constructed in a way that allows for certain provisions to be struck down without completely invalidating the entire piece of legislation.

Section 7: Protection from Foreign Born AI-Driven Psychological Programming

The development and deployment of AI systems by foreign entities, organizations or individuals shall be subject to the principles of transparency, explainability, fairness, privacy, and accountability as outlined in the above sections, and shall adhere to the standards established by NIST and their coauthored partners under this Act. The Secretary of State shall establish policies and procedures to ensure that foreign entities, organizations, and individuals seeking to develop or deploy AI systems in the United States comply with these principles and standards.

The use of AI systems by foreign entities, organizations or individuals that target or manipulate U.S. citizens with the intent to cause harm or undermine the security and integrity of the nation shall be prohibited, and may be subject to civil and criminal penalties but actions shall not fall short of military intervention when applicable. This includes the use of AI systems to spread disinformation, misinformation, interfere with elections, and incite violence or hatred against individuals or groups within the United States. The Department of Justice shall work in collaboration with other federal agencies to establish guidelines for identifying and prosecuting foreign entities, organizations, and individuals that violate this prohibition.

The Department of Homeland Security shall establish a process for monitoring the use of AI systems by foreign entities, organizations, and individuals within the United States, and shall report any suspicious activity to the appropriate federal agencies. The Department of Homeland Security shall also work in collaboration with the Federal Trade Commission to ensure that AI systems developed or deployed by foreign entities, organizations, and individuals comply with the principles of transparency, explainability, fairness, privacy, and accountability by adhering to the standards established by NIST and their coauthors under this Act.

The Department of State shall work in collaboration with foreign governments to promote the responsible and ethical development and deployment of AI systems, and shall establish partnerships and agreements with foreign entities, organizations, and individuals to share best practices and promote compliance with the principles and standards established under this Act. The Department of State shall also work in collaboration with other federal agencies to develop strategies for addressing threats to U.S. national security posed by the development and deployment of AI systems by foreign entities, organizations, and individuals.

The Department of Defense shall work to protect military infrastructure, its personnel and defense networks from attacks by foreign entities and their affiliates using AI systems. The Department of Defense shall work with all agencies listed to ensure our national defense and protect the American people from AI driven foreign psychological manipulation. The Secretary of State and the Department of Defense shall establish policies and procedures to ensure that AI systems developed or deployed by foreign entities, or their affiliates comply with these principles and standards. This includes, but is not limited to, AI systems used for military, intelligence, psychological programming of U.S. citizens and economic purposes.

Section 8: Protection from Foreign Born AI-Driven Psychological Programming, Specifically from the Government of the People's Republic of China (PRC)

The development and deployment of AI systems by foreign entities, organizations, or individuals, specifically the Government of the People's Republic of China (PRC), shall be subject to the principles of transparency, explainability, fairness, privacy, and accountability as outlined above, and shall adhere to the standards established by NIST with their coauthors under this Act. The Secretary of State and the Department of Defense shall establish policies and procedures to ensure that AI systems developed or deployed by the PRC or its affiliates comply with these principles and standards. This includes, but is not limited to, AI systems used for military, intelligence, psychological programming of U.S. citizens and economic purposes.

The use of AI systems by the PRC or its affiliates to target or manipulate U.S. citizens with the intent to cause harm or undermine the security and integrity of the nation shall be prohibited, and may be subject to civil and criminal penalties but actions shall not fall short of military intervention when applicable. This includes the use of AI systems to spread disinformation, misinformation, interfere with elections, and incite violence or hatred against individuals or

groups within the United States. The Department of Justice and the Department of Defense shall work in collaboration with other federal agencies to establish guidelines for identifying and prosecuting the PRC and its affiliates that violate this prohibition.

The Department of Homeland Security shall establish a process for monitoring the use of AI systems by the PRC and its affiliates within the United States, and shall report any suspicious activity to the appropriate federal agencies. The Department of Homeland Security shall also work in collaboration with the Federal Trade Commission and the Department of Defense to ensure that AI systems developed or deployed by the PRC and its affiliates comply with the principles of transparency, explainability, fairness, privacy, and accountability as outlined above, and adhere to the standards established by NIST and their coauthors under this Act. The Department of Defense shall work to protect military infrastructure, its personnel and defense networks from attacks by the PRC and their affiliates using AI systems and work with all agencies listed to ensure our national defense includes keeping the American people free from PRC AI driven psychological manipulation.

The Department of State shall work to promote the responsible and ethical development and deployment of AI systems by the PRC, and shall establish partnerships and agreements with the PRC, their organizations, and individuals to share best practices and promote compliance with the principles and standards established under this Act. The Department of State shall also work in collaboration with other federal agencies to develop strategies for addressing threats to U.S. national security posed by the development and deployment of AI systems by the PRC and its affiliates.

Section 9: Safeguarding First Amendment Rights

The development and deployment of AI systems must not infringe upon First Amendment rights, including freedom of speech, freedom of the press, and freedom of assembly, as well as the right to petition the government for redress of grievances. To this end, the following provisions shall be implemented:

(a) **Transparency and Accountability in AI-driven Content Moderation:** AI developers and deployers shall ensure that AI systems used for content moderation on online platforms operate in a transparent and accountable manner, and do not discriminate against or suppress lawful content based on political, religious, or ideological views. NIST, in collaboration with other federal agencies and stakeholders, shall establish standards for AI-driven content moderation that safeguard First Amendment rights while addressing legitimate concerns of national security, child safety and the prevention of online harassment that's deemed harmful.

(b) **Protection of Journalistic Integrity:** AI developers and deployers shall ensure that AI systems used in journalism do not undermine the integrity of the press or the free flow of information. This includes preventing the use of AI systems to generate or disseminate disinformation, deepfakes, or other misleading content that could infringe upon First Amendment rights or erode

public trust in journalism. NIST, in collaboration with other federal agencies and stakeholders, shall establish standards to protect journalistic integrity in the use of AI technologies.

(c) Ensuring the Right to Assembly and Petition: AI developers and deployers shall ensure that AI systems used in the context of public assembly and petitioning the government do not infringe upon the rights of individuals to engage in peaceful protests, demonstrations, or other forms of public expression. This includes preventing the use of AI systems for unwarranted surveillance or tracking of individuals participating in lawful public gatherings, as well as ensuring that AI systems do not facilitate the suppression or targeting of individuals based on their exercise of First Amendment rights. NIST, in collaboration with other federal agencies and stakeholders, shall establish standards to protect the right to assembly and petition in the context of AI technologies.

(d) Promoting Equal Expression and Diversity of Ideas and Viewpoints: AI developers and deployers shall ensure that AI systems used in the curation, recommendation, or distribution of information do not perpetuate echo chambers, filter bubbles, or otherwise contribute to the suppression of diverse ideas and viewpoints. The curation, recommendation, or distribution of information shall not be selective in such a way that supports a singular political agenda without the consumers informed consent. NIST, in collaboration with other federal agencies and stakeholders, shall establish standards to promote the equal expression and diversity of ideas and viewpoints in the use of AI technologies.

(e) Right to Contest AI Decisions: Individuals shall have the right to contest decisions made by AI systems that impact their First Amendment rights, including decisions related to content moderation, journalistic integrity, assembly and petition, and the promotion of diverse ideas and viewpoints. AI developers and deployers shall establish accessible and transparent mechanisms for individuals to contest such decisions in a timely manner and seek redress when appropriate.

(f) Ensuring AI Systems Do Not Violate First Amendment Rights: The FTC shall have the authority to investigate and enforce compliance with the provisions outlined in this section, and may impose civil penalties for violations. This will ensure that AI developers and deployers are held accountable for developing AI systems that infringe upon First Amendment rights. The FTC shall work in collaboration with NIST, other federal agencies, and stakeholders to enforce compliance with the standards established under this section.

Section 10: Protection of Constitutional Rights

Nothing in this Act shall be construed to infringe upon any rights or protections guaranteed by the Bill of Rights or the Constitution of the United States. The implementation and enforcement of this Act must always be carried out in accordance with the principles of the Constitution and the Bill of Rights, including, but not limited to, the First Amendment rights to freedom of speech, religion, press, assembly, and petition. Any interpretation, implementation, or enforcement action taken under this Act that is found to infringe upon the rights or protections guaranteed by the Bill of Rights or the Constitution of the United States shall be considered

invalid and subject to appropriate legal remedies. This Act is intended to protect the rights of American citizens and legal residents whose freedoms are protected and is not intended to protect foreign countries or their citizens who deploy AI systems within the United States.

Section 11: Effective Date

This Act shall take effect on the date of its enactment.