SENATE BILL NO. 212

INTRODUCED BY D. ZOLNIKOV

A BILL FOR AN ACT ENTITLED: "AN ACT GENERALLY REVISING LAWS RELATED TO TECHNOLOGY; CREATING THE RIGHT TO COMPUTE ACT; REQUIRING ~~SHUTDOWN CAPABILITIES~~ A RISK MANAGEMENT POLICY FOR CRITICAL INFRASTRUCTURE FACILITIES CONTROLLED BY AN ARTIFICIAL INTELLIGENCE SYSTEM; PROVIDING DEFINITIONS; AND PROVIDING AN IMMEDIATE EFFECTIVE DATE."

WHEREAS, innovations in computational technology, such as machine learning, enable technological breakthroughs in nearly every sector, leading to increased economic growth and greater prosperity; and

WHEREAS, ensuring the United States remains at the forefront of computational technology is critical for driving economic growth, safeguarding national security, and retaining a competitive edge over adversarial nations; and

WHEREAS, while recognizing the benefits of recent innovations in computational technologies, technology industry leaders have also expressed concern that some applications of powerful computational resources may pose a high risk to public health and safety; and

WHEREAS, federal and state governments increasingly propose far-reaching restrictions on the ability to privately own or make use of computational resources for lawful purposes, some of which may infringe on fundamental constitutional rights to property and free expression; and

WHEREAS, the Montana Legislature is the proper branch of government to establish policies and principles relating to the ability to own and make use of computational resources within the context of state constitutional provisions.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. **Section 1. Short title.** [Sections 1 through 7] may be cited as the "Right to Compute

Act".

NEW SECTION. **Section 2. Legislative findings -- intent.** The legislature finds that the rights to acquire, possess, and protect property under Article II, section 3, of the Montana constitution, and the freedom of expression under Article II, section 7, of the Montana constitution, also embody the notion of a fundamental right to own and make use of technological tools, including computational resources. Any restrictions placed by the government on the ability to privately own or make use of computational resources for lawful purposes must be limited to those demonstrably necessary and narrowly tailored to fulfill a compelling government interest ~~in public health or safety~~.

NEW SECTION. **Section 3. Right to compute.** Government actions that restrict the ability to privately own or make use of computational resources for lawful purposes, which infringes on citizens' fundamental rights to property and free expression, must be limited to those demonstrably necessary and narrowly tailored to fulfill a compelling government interest ~~in public health or safety~~.

NEW SECTION. **Section 4. Infrastructure controlled by critical artificial intelligence system ~~-- shutdown~~.** ~~(1)~~ When critical infrastructure facilities are controlled in whole or in part by ~~an~~ a critical artificial intelligence system, the deployer shall ~~ensure the capability to disable the artificial intelligence system's control over the infrastructure and revert to human control within a reasonable amount of time.~~

~~(2) When enacting a full shutdown, the deployer shall consider, as appropriate, disruptions to critical infrastructure that may result from a shutdown.~~

~~(3) Deployers shall implement, annually review, and test a risk management policy that includes a fallback mechanism and a redundancy and mitigation plan to ensure the deployer can continue operations and maintain control of the critical infrastructure facility without the use of the artificial intelligence system~~ develop a risk management policy after deploying the system that is reasonable and considers guidance and standards in the latest version of the artificial intelligence risk management framework from the national institute of standards and technology, the ISO/IEC 4200 artificial intelligence standard from the international organization

for standardization, or another nationally or internationally recognized risk management framework for artificial intelligence systems. A plan prepared under federal requirements constitutes compliance with this section.

NEW SECTION. **Section 5. Preservation of intellectual property.** Nothing in [sections 1 through 7] may be construed to alter, diminish, or interfere with the rights and remedies available under federal or state intellectual property laws, including but not limited to patent, copyright, trademark, and trade secret laws.

NEW SECTION. **Section 6. Preemption by federal law.** Nothing in [sections 1 through 7] may be construed to preempt federal laws.

NEW SECTION. **Section 7. Definitions.** As used in [sections 1 through 7], the following definitions apply:

(1) "Artificial intelligence system" means any machine learning-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including but not limited to content, decisions, predictions, and recommendations that can influence physical or virtual environments.

(2) "Compelling government interest ~~in public health or safety~~" means a government interest of the highest order in protecting the ~~health and safety of the~~ public that cannot be achieved through less restrictive means. This includes but is not limited to:

(a) ensuring that a critical infrastructure ~~facilities~~ facility controlled by an artificial intelligence system ~~can be shut down and the critical infrastructure facility can be returned to human control~~ develops a risk management policy;

(b) addressing conduct that deceives or defrauds the public;

(c) protecting individuals, especially minors, from harm by a person who distributes deepfakes and other harmful synthetic content with actual knowledge of the nature of that material; and

(d) taking actions that prevent or abate common law nuisances created by physical datacenter infrastructure.

(3) "Computational resources" means any tools, technologies, systems, or infrastructure, whether digital, analog, existing, or some other form, that facilitate any form of computation, data processing, storage, transmission, manipulation, control, creation, dissemination, or use of information and data. This includes but is not limited to hardware, software, algorithms, sensors, networks, protocols, platforms, services, systems, cryptography, machine learning, or quantum applications.

(3) (a) "Critical artificial intelligence" means an artificial intelligence system that is designed and deployed to make, or is a substantial factor in making, a consequential decision.

(b) The term does not include:

(i) an artificial intelligence system that is intended to:

(A) perform a narrow procedural task;

(B) improve the result of a previously completed human activity;

(C) perform a preparatory task to an assessment relevant to a consequential decision; or

(D) detect a decision-making pattern or a deviation from a preexisting decision-making pattern;

(ii) antifraud, antimalware, antivirus, calculator, cybersecurity, database, data storage, firewall, internet domain registration, internet-website loading, networking, robocall-filtering, spam-filtering, spell-checking, spreadsheet, web-caching, web-hosting, or search engine technologies or similar technologies; or

(iii) a technology that communicates in natural language for the purpose of providing users with information, makes referrals or recommendations, answers questions, or generates other content and that is subject to an acceptable use policy that prohibits the generation of unlawful content.

(4) "Critical infrastructure facility" has the same meaning as provided in 82-1-601.

(5) "Deployer" means an individual, company, or other organization that utilizes an artificial intelligence system.

(6) "Government actions" means any law, ordinance, regulation, rule, policy, ~~fee,~~ condition, test, permit, or administrative practice enacted by a government entity that restricts the common or intended use of computational resources by its owner or invitees.

(7) "Government entity" means any unit of state government including the state, counties, cities, towns, or political subdivisions, and any branch, department, division, office, or government entity of state or

local government.

NEW SECTION. **Section 8. Severability.** If a part of [this act] is invalid, all valid parts that are severable from the invalid part remain in effect. If a part of [this act] is invalid in one or more of its applications, the part remains in effect in all valid applications that are severable from the invalid applications.

NEW SECTION. **Section 9. Codification instruction.** [Sections 1 through 7] are intended to be codified as a new part of Title 2, chapter 10, and the provisions of Title 2, chapter 10, apply to [sections 1 through 7].

NEW SECTION. **Section 10. Effective date.** [This act] is effective on passage and approval.

- END -