# H.711

Introduced by Representatives Priestley of Bradford, Burrows of West Windsor, Chase of Chester, Christie of Hartford, Jerome of Brandon, Masland of Thetford, Roberts of Halifax, Sibilia of Dover, Sims of Craftsbury, Templeman of Brownington, White of Bethel, and Williams of Barre City

Referred to Committee on

Date:

Subject: Commerce and trade; consumer protection; liability for developers and deployers of artificial intelligence systems

Statement of purpose of bill as introduced: This bill proposes to create oversight and liability standards for developers and deployers of inherently dangerous artificial intelligence systems.

An act relating to creating oversight and liability standards for developers and deployers of inherently dangerous artificial intelligence systems

It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 9 V.S.A. chapter 63, subchapter 12 is added to read:

## Subchapter 12. Artificial Intelligence Oversight and Liability

### § 2495a. LEGISLATIVE INTENT

(a) Artificial intelligence systems are products that shift decision-making power and responsibility away from persons to software-based systems, often without direct human oversight. An artificial intelligence system can be inherently dangerous due to its capabilities, potential for misuse or exploitation, and ability to unilaterally evolve.

(b) Developers of sophisticated artificial intelligence systems have an obligation to make such systems safe when used in reasonably foreseeable ways. Deployers of these products also have an obligation to ensure that the products are safe and used in a way that does not materially affect an individual’s rights.

(c) In the artificial intelligence ecosystem, there will typically be multiple suppliers upstream of a consumer. The original developer of an artificial intelligence system should be responsible for harms attributable to the artificial intelligence system, even if the developer is not the deployer of the system to a consumer. Small businesses using off-the-shelf artificial intelligence products according to the product’s terms of use are not intended to be covered by this act.

### § 2495b. DEFINITIONS

As used in this subchapter:

(1) “Artificial intelligence system” means a machine-based system that can, for a given set of objectives, make predictions, recommendations, or

decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action.

(2) "Biometric data" means data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body. Biometric information includes depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures. Biometric information also includes data derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data had been derived.

(3) "Consequential decision" means a decision that either has a legal or similarly significant effect on an individual's access to the criminal justice system, housing, employment, credit, education, health care, or insurance.

(4) "Consumer" means any individual who is a resident of this State.

(5) "Deployer" means a person, including a developer, who uses or operates an artificial intelligence system for internal use or for use by third parties in the State.

(6) “Developer” means a person who designs, codes, produces, owns, or substantially modifies an artificial intelligence system for internal use or for use by a third party in the State.

(7) “Dual-use foundational model” means an artificial intelligence system that:

(A) is trained on broad data;

(B) generally uses self-supervision;

(C) contains at least 10 billion parameters;

(D) is applicable across a wide range of contexts; and

(E) exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to economic security, public health or safety, or any combination of those matters, such as by:

(i) substantially lowering the barrier of entry for nonexperts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;

(ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or

(iii) permitting the evasion of human control or oversight through means of deception or obfuscation.

(8) “Generative artificial intelligence system” means an artificial intelligence system that is capable of generating output including text, imagery, audio, and synthetic data.

(9) “High-risk artificial intelligence system” means any artificial intelligence system, regardless of the number of parameters and supervision structure, that is:

(A) used, reasonably foreseeable as being used, or is a controlling factor in making a consequential decision;

(B) used, or reasonably foreseeable as being used, to categorize groups of persons by sensitive and protected characteristics, such as race, ethnic origin, or religious belief;

(C) used, or reasonably foreseeable as being used, in the direct management or operation of critical infrastructure;

(D) used, or reasonably foreseeable as being used, in vehicles, medical devices, or in the safety system of a product;

(E) used, or reasonably foreseeable as being used, to influence elections or voters; or

(F) used to collect the biometric data of an individual from a biometric identification system without consent.

(10) "Inherently dangerous artificial intelligence system" means a high-risk artificial intelligence system, dual-use foundational model, or generative artificial intelligence system.

## § 2495c. OVERSIGHT AND ENFORCEMENT

(a) The Division of Artificial Intelligence within the Agency of Digital Services shall collect and review Artificial Intelligence Safety and Impact Assessments pursuant to this subchapter.

(b) The Attorney General shall enforce the provisions of this subchapter and may bring an action in the name of the State against a deployer or developer for noncompliance to restrain by temporary or permanent injunction the noncompliance. The action may be brought in the Superior Court of the county in which such person resides, has a place of business, or is doing business. Said courts are authorized to issue temporary or permanent injunctions to restrain and prevent violations of this subchapter, such injunctions to be issued without bonds, or to dissolve, or revoke the certificate of authority of, a deployer or developer.

## § 2495d. ARTIFICIAL INTELLIGENCE SYSTEM SAFETY AND IMPACT ASSESSMENT

(a) Each deployer of an inherently dangerous artificial intelligence system shall:

(1) submit to the Division of Artificial Intelligence an Artificial Intelligence System Safety and Impact Assessment prior to deploying the inherently dangerous artificial intelligence system in this State, and every two years thereafter; and

(2) submit to the Division of Artificial Intelligence an updated Artificial Intelligence System Safety and Impact Assessment if the deployer makes a material and substantial change to the inherently dangerous artificial intelligence system that includes:

(A) the purpose for which the system is used for; or

(B) the type of data the system processes or uses for training purposes.

(b) Each Artificial Intelligence System Impact Assessment pursuant to subsection (a) of this section shall include, with respect to the inherently dangerous artificial intelligence system:

(1) the purpose of the system;

(2) the deployment context and intended use cases;

(3) the benefits of use;

(4) any foreseeable risk of unintended or unauthorized uses and the steps taken, to the extent reasonable, to mitigate such risk;

(5) whether the model is proprietary;

(6) a description of the data the system processes or uses for training purposes;

(7) a description of transparency measures, including identifying to individuals when the system is in use;

(8) identification of any third-party artificial intelligence systems or datasets the deployer relies on to train or operate the system, if applicable;

(9) whether the developer of the system, if different than the deployer, disclosed the information pursuant to subsection 2495e(b) of this chapter as well as the results of testing, vulnerabilities, and the parameters for safe and intended use;

(10) a description of the data the system, once deployed, processes as inputs;

(11) a description of postdeployment monitoring and user safeguards, including a description of the oversight process in place to address issues as issues arise; and

(12) a description of how the model impacts consequential decisions or the collection of biometric data.

(c) Each deployer of a high-risk artificial intelligence system must submit a one-, six-, and 12-month testing result to the Division of Artificial Intelligence showing the reliability of the results generated by the system, any variance in those results over the testing periods, and any mitigation strategies for variances, in the first year of deployment.

(d) Upon the Division of Artificial Intelligence receiving notice that a deployer of an inherently dangerous artificial intelligence system is not in compliance with the requirements under this section, the Division shall immediately notify the deployer of the finding in writing and order the deployer to submit the assessment required pursuant to subsection (a) of this section. If the deployer fails to submit the assessment within 45 days after receiving the notice, the Division of Artificial Intelligence shall notify the Attorney General in writing of the violation.

### § 2495e. STANDARD OF CARE

(a) Each developer or deployer of any inherently dangerous artificial intelligence system that could be reasonably expected to impact consumers shall exercise reasonable care to avoid any reasonably foreseeable risk arising out of the development, intentional and substantial modification, or deployment of an artificial intelligence system that causes or is likely to cause:

(1) the commission of a crime or unlawful act;

(2) any unfair or deceptive treatment of or unlawful impact on an individual;

(3) any physical, financial, relational, or reputational injury on an individual;

(4) psychological injuries that would be highly offensive to a reasonable person;

(5) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of a person if such intrusion would be offensive to a reasonable person;

(6) any violation to the intellectual property rights of persons under applicable State and federal laws;

(7) discrimination on the basis of a person’s or class of person’s actual or perceived race, color, ethnicity, sex, sexual orientation, gender identity, sex characteristics, religion, national origin, familial status, biometric information, or disability status;

(8) distortion of a person’s behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm; or

(9) the exploitation of the vulnerabilities of a specific group of persons due to their age or physical or mental disability in order to materially distort the behavior of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm.

(b) Each developer of an inherently dangerous artificial intelligence system shall:

(1) document and disclose to any actual or potential deployer of the artificial intelligence system any reasonably foreseeable risk, including by

unintended or unauthorized uses, that causes or is likely to cause any of the injuries as set forth in subsection (a) of this section; and

(2) document and disclose to any actual or potential deployer of the artificial intelligence system any risk mitigation processes that are reasonably foreseeable to mitigate any injury as set forth in subsection (a) of this section.

### § 2495f. UNSAFE ARTIFICIAL INTELLIGENCE PRODUCTS, PROHIBITIONS

(a) No developer shall offer, sell, lease, give, or otherwise place in the stream of commerce:

(1) an inherently dangerous artificial intelligence system, unless the developer has conducted a documented testing, evaluation, verification, and validation of that system at least as stringent as the latest version of the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology (NIST); or

(2) an artificial intelligence system that creates reasonably foreseeable risks pursuant to section 2495e of this chapter, unless the developer mitigates these risks to the extent possible, considers alternatives, and discloses vulnerabilities and mitigation tactics to a deployer.

(b) No deployer shall deploy an inherently dangerous artificial intelligence system or an artificial intelligence system that creates reasonably foreseeable risks pursuant to section 2495e of this chapter unless the deployer has designed and implemented a risk management policy and program for such model or system. The risk management policy shall specify the principles, processes, and personnel that the deployer shall use in maintaining the risk management program to identify, mitigate, and document any risk that is a reasonably foreseeable consequence of deploying or using such system. Each risk management policy and program designed, implemented, and maintained pursuant to this subsection shall be:

(1) at least as stringent as the latest version of the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology (NIST); and

(2) reasonable considering:

(A) the size and complexity of the deployer;

(B) the nature and scope of the system, including the intended uses and unintended uses and the modifications made to the system by the deployer; and

(C) the data that the system, once deployed, processes as inputs.

### § 2495g. VIOLATIONS; PRIVATE RIGHT OF ACTION

(a) A person who violates this subchapter or rules adopted under this subchapter commits an unfair practice in commerce in violation of section 2453 of this title.

(b) A consumer harmed by a violation of this subchapter or rules adopted under this subchapter may bring an action in Superior Court for damages incurred, injunctive relief, punitive damages in the case of an intentional violation, and reasonable costs and attorney’s fees.

### § 2495h. LIMITATIONS

(a) In any civil action brought against a deployer or developer pursuant to section 2495g of this chapter, there shall be a rebuttable presumption that a developer or deployer upheld the standard of care if the developer or deployer complied with the provisions of this subchapter.

(b) A deployer who is not also the developer of an inherently dangerous artificial intelligence system shall not be found in violation of this subchapter if the deployer deploys such a system in accordance with the developer’s instructions and information as set forth in section 2495e of this chapter.

(c) Nothing in this subchapter shall restrict a developer’s or deployer’s ability to:

(1) comply with federal, State, or municipal ordinances or regulations;

(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, State, municipal, or other governmental authorities;

(3) investigate, establish, exercise, prepare for, or defend legal claims;

(4) provide a product or service specifically requested by a consumer;

(5) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(6) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or by similar independent oversight entities that determine:

(A) that the expected benefits of the research outweigh the risks associated with such research; and

(B) that the developer or deployer has implemented reasonable safeguards to mitigate the risks associated with such research; or

(7) assist another developer or deployer with any of the obligations imposed under this subchapter.

Sec. 2. EFFECTIVE DATE

This act shall take effect on July 1, 2024.