H.710

Introduced by Representatives Priestley of Bradford, Anthony of Barre City, 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: Information technology; artificial intelligence; developers; deployers

Statement of purpose of bill as introduced: This bill proposes to regulate developers and deployers of high-risk artificial intelligence systems and developers of generative artificial intelligence systems.

An act relating to regulating developers and deployers of certain artificial intelligence systems

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

Sec. 1. 22 V.S.A. chapter 17 is added to read:

CHAPTER 17. ARTIFICIAL INTELLIGENCE

§ 1001. DEFINITIONS

As used in this chapter:

(1) "Algorithmic discrimination" means an automated system's

contribution to unjustified differential treatment or impacts that disfavor individuals or groups of individuals based on their race, color, ethnicity, sex, sexual orientation, gender identity, religion, age, national origin, limited English proficiency, disability, veteran status, genetic information, or any other classification protected by State or federal law.

(2) "Artificial intelligence" means any technology, including machine learning, that uses data to train an algorithm or predictive model for the purpose of enabling a computer system or service to autonomously perform any task, including visual perception, language processing, and speech recognition, that is normally associated with human intelligence or perception.

(3) "Artificial intelligence system" means any computer system or service that incorporates or uses artificial intelligence.

(4) "Consequential decision" means any decision that has a material legal, or similarly significant, effect on a consumer's access to credit, criminal justice, education, employment, health care, housing, or insurance.

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

(6) "Deployer" means any person who deploys or uses a high-risk artificial intelligence system to make a consequential decision.

(7) "Developer" means any person who develops or who intentionally and substantially modifies:

(A) a high-risk artificial intelligence system; or

(B) a generative artificial intelligence system.

(8) "Digital watermark" means information that:

(A) is embedded in, and reasonably difficult to remove from, any digital content; and

(B) enables a consumer who accesses the digital content to verify the authenticity of the digital content and to determine whether the digital content is synthetic digital content.

(9) "Foundation model" means any form of artificial intelligence that:

(A) is trained on broad data at scale;

(B) is designed for generality of output; and

(C) can be adapted to a wide range of distinctive tasks.

(10) "Generative artificial intelligence" means any form of artificial intelligence, including a foundation model, that is able to produce synthetic digital content, including audio, images, text, and videos.

(11) "Generative artificial intelligence system" means any computer system or service that incorporates or uses generative artificial intelligence.

(12) "High-risk artificial intelligence system" means any artificial intelligence system that, when deployed, makes or is a controlling factor in making a consequential decision.

(13) "Machine learning" means any technique that enables a computer system or service to autonomously learn and adapt by using algorithms and

statistical models to autonomously analyze and draw inferences from patterns in data.

(14) "Red teaming" means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI.

(15) "Search engine" means any computer system or service that searches for, and identifies, items in a database that correspond to keywords or characters specified by a consumer, and is offered to, or used by, any consumer.

(16) "Search engine operator" means any person who owns or controls a search engine.

(17) "Significant update" means any new version, new release, or other update to a high-risk artificial intelligence system that results in significant changes to such high-risk artificial intelligence system's use case, key functionality, or expected outcomes.

(18)(A) "Social media platform" means a public or semipublic internet-based service or application that:

(i) is used by a consumer;

(ii) is primarily intended to connect and allow users to socially interact within the service or application; and

(iii) enables a consumer to:

(I) construct a public or semipublic profile for the purposes of signing into and using the service or application;

(II) populate a public list of other persons with whom the consumer shares a social connection within the service or application; and

(III) create or post content that is viewable by other persons, including on message boards, in chat rooms, or through a landing page or main feed that presents the consumer with content generated by other persons.

(B) "Social media platform" does not include a public or semipublic internet-based service or application that:

(i) exclusively provides e-mail or direct messaging services;

(ii) primarily consists of news, sports, entertainment, interactive video games, electronic commerce, or content that is preselected by the provider or for which any chat, comments, or interactive functionality is incidental to, directly related to, or dependent on the provision of such content; or

(iii) is used by and under the direction of an educational entity, including a learning management system or a student engagement program.

(19) "Social media platform operator" means any person who owns or controls a social media platform.

(20) "Synthetic digital content" means any digital content, including any audio, image, text, or video, that is produced by a generative artificial

intelligence system.

(21) "Trade secret" has the same meaning as in 9 V.S.A. § 4601.

§ 1002. DUTIES OF DEVELOPERS OF HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEMS

(a) Each developer shall use reasonable care to avoid any risk of algorithmic discrimination that is a reasonably foreseeable consequence of developing, or intentionally and substantially modifying, a high-risk artificial intelligence system to make a consequential decision. In any enforcement action brought by the Attorney General pursuant to section 1007 of this chapter, there shall be a rebuttable presumption that a developer used reasonable care as required under this subsection if the developer complied with the provisions of this section.

(b) Except as provided in subsection (e) of this section, no developer of a high-risk artificial intelligence system shall offer, sell, lease, give, or otherwise provide a high-risk artificial intelligence system to a deployer unless the developer provides to the deployer all of the following:

(1) a statement disclosing the intended uses of the high-risk artificial intelligence system;

(2) documentation disclosing:

(A) the known limitations of the high-risk artificial intelligence system, including any and all reasonably foreseeable risks of algorithmic

discrimination arising from the intended uses of the high-risk artificial intelligence system;

(B) the purpose of the high-risk artificial intelligence system and the intended benefits, uses, and deployment contexts of the high-risk artificial intelligence system;

(C) a summary of the type of data collected from individuals and processed by the high-risk artificial intelligence system when the high-risk artificial intelligence system is used to make a consequential decision; and

(D) an analysis of any adverse impact that the deployer's deployment or use of the high-risk artificial intelligence system will potentially have on any individual, or group of individuals, on the basis of race, color, ethnicity, sex, sexual orientation, gender identity, religion, age, national origin, limited English proficiency, disability, or veteran status.

(3) documentation describing:

(A) the type of data used to program or train the high-risk artificial intelligence system;

(B) how the high-risk artificial intelligence system was evaluated for validity and explainability before the high-risk artificial intelligence system was licensed or sold;

(C) the data governance measures used to cover the training data sets and the measures used to examine the suitability of data sources, possible

biases, and appropriate mitigation;

(D) the outputs of the high-risk artificial intelligence system and how these outputs may be used to make consequential decisions;

(E) the measures the developer has taken to mitigate any risk of algorithmic discrimination that the developer knows may arise from deployment or use of the high-risk artificial intelligence system; and

(F) how an individual can use the high-risk artificial intelligence system to make, or monitor the high-risk artificial intelligence system when the high-risk artificial intelligence system is deployed or used to make, a consequential decision.

(c) Except as provided in subsection (e) of this section, each developer that offers, sells, leases, gives, or otherwise provides to a deployer a high-risk artificial intelligence system shall provide to the deployer the technical capability to access, or otherwise make available to the deployer, all information and documentation in the developer's possession, custody, or control that the deployer reasonably requires to complete an impact assessment pursuant to subsection 1003(c) of this chapter.

(d) Each developer shall post a clear and conspicuous statement on its public-facing website summarizing:

(1) the types of high-risk artificial intelligence systems that:

(A) the developer has developed or has intentionally and

substantially modified; and

(B) are currently deployed or used by a deployer; and

(2) how the developer manages any reasonably foreseeable risk of algorithmic discrimination that may arise from deployment or use of each high-risk artificial intelligence system described in subdivision (1) of this subsection.

(e) Nothing in subsections (b)–(d) of this section shall be construed to require a developer to disclose any trade secret.

(f)(1) The Attorney General may require that a developer disclose to the Attorney General any statement or documentation described in subsection (b) of this section if the statement or documentation is relevant to an investigation conducted by the Attorney General.

(2) The Attorney General may evaluate any statement or documentation to ensure compliance with the provisions of this section, and any such statement or documentation is exempt from public inspection and copying under the Public Records Act.

(3) To the extent any information contained in any such statement or documentation includes any information subject to the attorney-client privilege or work product protection, disclosure to the Attorney General pursuant to this subsection shall not constitute a waiver of that privilege or protection.

§ 1003. DUTIES OF DEPLOYERS OF HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEMS

(a) Each deployer shall use reasonable care to avoid any risk of algorithmic discrimination that is a reasonably foreseeable consequence of deploying or using a high-risk artificial intelligence system to make a consequential decision. In any enforcement action brought by the Attorney General pursuant to section 1007 of this chapter, there shall be a rebuttable presumption that a deployer used reasonable care as required under this subsection if the deployer complied with the provisions of this section.

(b) No deployer shall deploy or use a high-risk artificial intelligence system to make a consequential decision unless the deployer has designed and implemented a risk management policy and program for the high-risk artificial intelligence 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 of algorithmic discrimination that is a reasonably foreseeable consequence of deploying or using such high-risk artificial intelligence system to make a consequential decision. 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 or another nationally or internationally recognized risk management framework for artificial intelligence systems; and

(2) reasonable, considering:

(A) the size and complexity of the deployer;

(B) the nature and scope of the high-risk artificial intelligence systems deployed and used by the deployer, including the intended uses of those systems;

(C) the sensitivity and volume of data processed in connection with the high-risk artificial intelligence systems deployed and used by the deployer; and

(D) the cost to the deployer to implement and maintain the risk management program.

(c)(1) Except as provided in subdivisions (3) and (4) of this subsection, no deployer shall deploy or use a high-risk artificial intelligence system to make a consequential decision unless the deployer has completed an impact assessment for the high-risk artificial intelligence system. The deployer shall complete an impact assessment for a high-risk artificial intelligence system:

(A) before the deployer initially deploys the high-risk artificial intelligence system;

(B) not later than 45 days following the close of each calendar year during which the deployer used the high-risk artificial intelligence system to

make a consequential decision; and

(C) not later than 45 days after each significant update to the high-risk artificial intelligence system by the deployer or developer.

(2) Each impact assessment completed pursuant to this subsection shall include, at a minimum:

(A) a statement by the deployer disclosing:

(i) the purpose, intended use cases, and deployment context of, and benefits afforded by, the high-risk artificial intelligence system; and

(ii) whether the deployment or use of the high-risk artificial intelligence system poses a reasonably foreseeable risk of algorithmic discrimination and, if so:

(I) the nature of the algorithmic discrimination; and

(II) the steps that have been taken, to the extent feasible, to mitigate the risk;

(B) for each post-deployment impact assessment completed pursuant to this subsection (c), the extent to which the high-risk artificial intelligence system was used in a manner that was consistent with, or varied from, the developer's intended uses of the high-risk artificial intelligence system;

(C) a description of:

(i) the data the high-risk artificial intelligence system processes as inputs; and

(ii) the outputs the high-risk artificial intelligence system produces;

(D) if the deployer used data to retrain the high-risk artificial intelligence system, an overview of the type of data the deployer used to retrain the high-risk artificial intelligence system;

(E) any metrics used to evaluate the performance and known limitations of the high-risk artificial intelligence system;

(F) a description of any transparency measures taken concerning the high-risk artificial intelligence system, including any measure taken to disclose to a consumer in this State that the high-risk artificial intelligence system is in use when the high-risk artificial intelligence system is in use; and

(G) a description of any postdeployment monitoring performed, and user safeguards provided, concerning the high-risk artificial intelligence system, including any oversight process established by the deployer to address issues arising from deployment or use of the high-risk artificial intelligence system as such issues arise.

(3) A single impact assessment may address a comparable set of high-risk artificial intelligence systems deployed or used by a deployer.

(4) If a deployer completes an impact assessment for the purpose of complying with another applicable law or regulation, that impact assessment shall be deemed to satisfy the requirements established in this subsection if the

impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be completed pursuant to this subsection.

(5) A deployer who completes an impact assessment pursuant to this subsection shall maintain the impact assessment, and all records concerning the impact assessment, for a reasonable period of time, but not less than three years.

(d) Not later than the time that a deployer uses a high-risk artificial intelligence system to make a consequential decision concerning an individual, the deployer shall:

(1) notify the individual that the deployer is using a high-risk artificial intelligence system to make the consequential decision concerning the individual; and

(2) provide to the individual:

(A) a statement disclosing the purpose of the high-risk artificial intelligence system;

(B) contact information for the deployer; and

(C) a description, in plain language, of the high-risk artificial intelligence system, which shall include a description of any and all human components and how any and all automated components are used to inform the consequential decision.

(e) Each deployer shall post a clear and conspicuous statement on its

public-facing website summarizing:

(1) the types of high-risk artificial intelligence systems that are currently deployed or used by a deployer; and

(2) how the deployer manages any reasonably foreseeable risk of algorithmic discrimination that may arise from use or deployment of each high-risk artificial intelligence system described in subdivision (1) of this subsection.

(f) Nothing in subsections (b)–(e) of this section shall be construed to require a deployer to disclose any trade secret.

(g)(1) The Attorney General may require that a deployer disclose to the Attorney General any risk management policy designed and implemented pursuant to subsection (b) of this section, impact assessment completed pursuant to subsection (c) of this section, or record maintained pursuant to subdivision (c)(5) of this section if the risk management policy, impact assessment, or record is relevant to an investigation conducted by the Attorney General.

(2) The Attorney General may evaluate the risk management policy, impact assessment, or record to ensure compliance with the provisions of this section, and any such risk management policy, impact assessment, or record is exempt from public inspection and copying under the Public Records Act.

(3) To the extent any information contained in any such risk

management policy, impact assessment, or record includes any information subject to the attorney-client privilege or work product protection, disclosure to the Attorney General pursuant to this subsection shall not constitute a waiver of that privilege or protection.

§ 1004. DUTIES OF DEVELOPERS OF GENERATIVE ARTIFICIAL INTELLIGENCE SYSTEMS

(a)(1) Each developer shall use reasonable care to avoid any reasonably foreseeable risk arising out of any development or any intentional and substantial modification of a generative artificial intelligence system:

(A) of any unfair or deceptive treatment of, or unlawful disparate impact on, consumers in this State;

(B) of any emotional, financial, mental, physical, or reputational injury to consumers in this State;

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

(D) to the intellectual property rights of persons under applicable State and federal intellectual property laws.

(2) In any enforcement action brought by the Attorney General pursuant to section 1007 of this chapter, there shall be a rebuttable presumption that a developer used reasonable care as required under subdivision (1) of this

subsection if the developer complied with the provisions of this section.

(b)(1) No developer who develops, or who intentionally and substantially modifies, a generative artificial intelligence system on or after October 1, 2024 shall offer, sell, lease, give, or otherwise provide the generative artificial intelligence system to any consumer in this State, or to any person doing business in this State, unless the generative artificial intelligence system satisfies the requirements established in this subsection.

(2) Each generative artificial intelligence system described in subdivision (1) of this subsection shall:

(A) reduce and mitigate the reasonably foreseeable risks described in subdivision (a)(1) of this section through efforts such as the involvement of independent experts and documentation of any reasonably foreseeable, but nonmitigable, risks;

(B) exclusively incorporate and process datasets that are subject to data governance measures that are appropriate for generative artificial intelligence systems, including data governance measures to examine the suitability of data sources for possible biases and appropriate mitigation;

(C) achieve, throughout the lifecycle of the generative artificial intelligence system, appropriate levels of performance, predictability, interpretability, corrigibility, safety, and cybersecurity, as assessed through appropriate methods, including model evaluation involving independent

experts, documented analysis, and extensive testing, during conceptualization, design, and development of the generative artificial intelligence system; and

(D) incorporate science-backed standards and techniques that:

(i) authenticate and track the provenance of digital content;

(ii) detect synthetic digital content;

(iii) label synthetic digital content by using a digital watermark or other mechanism; and

(iv) prevent the generative artificial intelligence system from producing imagery that would constitute child sexual abuse materials under 13 V.S.A. § 2827 if an actual child was involved in the creation of the imagery, or imagery of an identifiable person who is nude, as defined in 13 V.S.A. § 2606, or who is engaged in sexual conduct, as defined in 13 V.S.A. § 2821, without the person's consent.

(3) A developer who develops, or who intentionally and substantially modifies, a generative artificial intelligence system described in subdivision (1) of this subsection shall maintain all records related to the purposes set forth in this subsection for a reasonable period of time, but not less than three years.

(c)(1) Except as provided in subdivisions (3) and (4) of this subsection, no developer who develops, or who intentionally and substantially modifies, a generative artificial intelligence system on or after October 1, 2024 shall offer, sell, lease, give, or otherwise provide the generative artificial intelligence

system to any consumer in this State, or any person doing business in this State, unless the developer has completed an impact assessment for the generative artificial intelligence system pursuant to this subsection.

(2) Each impact assessment completed pursuant to this subsection shall include, at a minimum, an evaluation of:

(A) the intended purpose of the generative artificial intelligence system;

(B) the extent to which the generative artificial intelligence system has been, or is likely to be, used;

(C) the extent to which any prior use of the generative artificial intelligence system has harmed the health or safety of individuals, adversely impacted the fundamental rights of individuals, or given rise to significant concerns relating to the materialization of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to authorities of competent jurisdiction;

(D) the potential extent to which use of the generative artificial intelligence system may harm the health and safety of individuals or adversely impact the fundamental rights of individuals, including the intensity of the potential harm or adverse impact and the number of individuals likely to suffer the harm or adverse impact;

(E) the extent to which individuals who may be harmed or adversely

impacted by the generative artificial intelligence system are dependent on the outcomes produced by the generative artificial intelligence system for reasons such as the legal or practical challenges of opting out of those outcomes;

(F) the extent to which individuals who may be harmed or adversely impacted by users of the generative artificial intelligence system are comparatively more vulnerable to experiencing those harms or impacts due to factors such as an age imbalance, economic or social circumstances, knowledge, or power; and

(G) the extent to which the outcomes produced by the generative artificial intelligence system, other than outcomes affecting health and safety, are easily reversible.

(3) A single impact assessment may address a comparable set of generative artificial intelligence systems developed, or intentionally and substantially modified, by a developer.

(4) If a developer completes an impact assessment for the purpose of complying with another applicable law or regulation, that impact assessment shall be deemed to satisfy the requirements established in this subsection if the impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be completed pursuant to this subsection.

(5) A developer who completes an impact assessment pursuant to this subsection shall maintain the impact assessment, and all records concerning the

impact assessment, for a reasonable period of time, but not less than three years.

(d) Each developer that offers, sells, leases, gives, or otherwise provides any generative artificial intelligence system described in subsections (b) and (c) of this section to any search engine operator or social media platform operator shall provide to the search engine operator or social media platform operator the technical capability that the search engine operator or social media platform operator reasonably requires to perform the search engine operator's or social media platform operator's duties under section 1005 of this chapter. Nothing in this subsection shall be construed to require a developer to disclose any trade secret.

(e)(1) The Attorney General may require that a developer disclose to the Attorney General any record maintained pursuant to subdivision (b)(3) of this section, impact assessment completed pursuant to subsection (c) of this section, or record maintained pursuant to subdivision (c)(5) of this section if the impact assessment or record is relevant to an investigation conducted by the Attorney General.

(2) The Attorney General may evaluate the impact assessment or record to ensure compliance with the provisions of this section, and any such impact assessment or record is exempt from public inspection and copying under the Public Records Act.

(3) To the extent any information contained in any such impact assessment or record includes any information subject to the attorney-client privilege or work product protection, disclosure to the Attorney General pursuant to this subsection shall not constitute a waiver of that privilege or protection.

§ 1005. SIGNAL INDICATING CONTENT LIKELY PRODUCED BY GENERATIVE ARTIFICIAL INTELLIGENCE

Each search engine or social media platform that is offered to or used by any consumer in this State to access any digital content that the search engine operator or social media platform operator knows, or reasonably believes, is synthetic digital content shall provide to the consumer a signal indicating that the digital content was produced, or is reasonably believed to have been produced, by generative artificial intelligence. The signal shall be available to the consumer at all times that the consumer is consuming the digital content on the search engine or social media platform.

§ 1006. OTHER RIGHTS UNAFFECTED

(a) Nothing in this chapter shall be construed to restrict a developer's, deployer's, search engine operator's, or social media platform operator's ability to:

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

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

(3) cooperate with law enforcement agencies concerning conduct or activity that the developer, deployer, search engine operator, or social media platform operator reasonably and in good faith believes may violate federal, State, or municipal ordinances, rules, or regulations;

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

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

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

(7) take steps at the request of a consumer prior to entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of a consumer or another individual;

(9) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such actions;

(10) 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 similar independent oversight entity that determines:

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

(B) whether the developer, deployer, search engine operator, or social media platform operator has implemented reasonable safeguards to mitigate the risks associated with the research;

(11) assist another developer, deployer, search engine operator, or social media platform operator with any of the obligations imposed under this chapter; or

(12) take any action that is in the public interest in the areas of public health, community health, or population health, but solely to the extent that the action is subject to suitable and specific measures to safeguard the public.

(b) The obligations imposed on developers, deployers, search engine operators, and social media platform operators under this chapter shall not restrict a developer's, deployer's, search engine operator's, or social media platform operator's ability to:

(1) conduct internal research to develop, improve, or repair products, services, or technologies;

(2) effectuate a product recall;

(3) identify and repair technical errors that impair existing or intended

functionality; or

(4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the developer, deployer, search engine operator, or social media platform operator.

(c) The obligations imposed on developers, deployers, search engine operators, and social media platform operators under this chapter shall not apply in the event that compliance by the developer, deployer, search engine operator, or social media platform operator with any such obligation would violate an evidentiary privilege under the laws of this State.

(d) If a developer, deployer, search engine operator, or social media platform operator engages in any action pursuant to an exemption set forth in this section, the developer, deployer, search engine operator, or social media platform operator bears the burden of demonstrating that the action qualifies for the exemption.

§ 1007. ENFORCEMENT

(a) The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

(b)(1) Except as provided in subsection (f) of this section, during the period from October 1, 2024 through March 31, 2026, the Attorney General shall, prior to initiating any action for a violation of any provision of this chapter,

issue a notice of violation to the developer, deployer, search engine operator, or social media platform operator if the Attorney General determines that a cure is possible. If the developer, deployer, search engine operator, or social media platform operator fails to cure the violation within 60 days following receipt of the notice of violation, the Attorney General may bring an action pursuant to this section.

(2) Not later than January 1, 2025, the Attorney General shall submit a report to the General Assembly disclosing:

(A) the number of notices of violation the Attorney General has issued;

(B) the nature of each violation;

(C) the number of violations that were cured during the 60-day cure period; and

(D) any other matter the Attorney General deems relevant to the purposes of the report.

(c) Except as provided in subsection (f) of this section, beginning on April 1, 2026, the Attorney General may issue a notice of violation and provide a developer, deployer, search engine operator, or social media platform operator the opportunity to cure an alleged violation of this chapter prior to initiating an action. In determining whether to provide an opportunity to cure, the Attorney General may consider:

(1) the number of violations;

(2) the size and complexity of the developer, deployer, search engine operator, or social media platform operator;

(3) the nature and extent of the developer's, deployer's, search engine operator's, or social media platform operator's business;

(4) the substantial likelihood of injury to the public;

(5) the safety of persons or property; and

(6) whether the alleged violation or violations were likely caused by human or technical error.

(d) Nothing in this chapter shall be construed to create a private right of action for violations of this chapter or of any other law.

(e) Except as provided in subsection (f) of this section, a person who violates the requirements of this chapter commits an unfair and deceptive act in trade and commerce in violation of 9 V.S.A. § 2453. The Attorney General has the same authority to make rules, conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as is provided under 9 V.S.A. chapter 63, the Vermont Consumer Protection Act.

(f)(1) Notwithstanding any provision of this section to the contrary, the Attorney General shall not commence any action against a developer, deployer, search engine operator, or social media platform operator to enforce the provisions of this chapter if:

(A) the high-risk artificial intelligence system, generative artificial intelligence system, search engine, or social media platform, as applicable, is in compliance with the latest version of the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology or another nationally or internationally recognized risk management framework for artificial intelligence systems; and

(B) the developer, deployer, search engine operator, or social media platform operator:

(i) encourages the deployers or users of the high-risk artificial intelligence system, generative artificial intelligence system, search engine, or social media platform, as applicable, to provide feedback to the appropriate developer, deployer, search engine operator, or social media platform operator;

(ii) as a result of the feedback described in subdivision (i) of this subdivision (1)(B), discovers a violation of any provision of this chapter; and

(iii) not later than 30 days after discovering the violation as set forth in subdivision (ii) of this subdivision (1)(B), takes both of the following actions:

(I) cures the violation by utilizing red teaming to test the high-risk artificial intelligence system, generative artificial intelligence system, search engine, or social media platform, as applicable; and

(II) notifies the Attorney General, in a form and manner

prescribed by the Attorney General, that the violation has been cured.

(2) The developer, deployer, search engine operator, or social media platform operator bears the burden of demonstrating to the Attorney General that the requirements established in subdivision (1) of this subsection have been satisfied.

Sec. 2. 13 V.S.A. § 2606 is amended to read:

§ 2606. DISCLOSURE OF SEXUALLY EXPLICIT IMAGES WITHOUT CONSENT

(a) As used in this section:

* * *

(5) "Visual image" includes a photograph, film, videotape, recording, synthetic image partially or fully generated by a computer system, or digital reproduction.

* * *

Sec. 3. EFFECTIVE DATE

This act shall take effect on July 1, 2024.