OLR Bill Analysis

sSB 2 (File 188, as amended by Senate "A" and "B")*

AN ACT CONCERNING ARTIFICIAL INTELLIGENCE.

TABLE OF CONTENTS:

provides certain affirmative defenses; and deems violations CUTPA violations, but does not provide a private right of action

§ 8 — CONNECTICUT ACADEMY OF SCIENCE AND ENGINEERING (CASE) LIAISONS

Allows legislative leaders to request CASE members to serve as a liaison between the academy and state government; requires liaisons to serve certain purposes, such as designing tools to determine compliance with the bill's requirements and evaluating the adoption of AI systems by businesses

§ 9 — ELECTIONS AND DECEPTIVE AI MEDIA

Generally makes it a crime for a person (e.g., individual or entity) to knowingly distribute a communication with deceptive synthetic media within 90 days before an election or primary

§ 10 — UNLAWFUL DISSEMINATION OF AN INTIMATE IMAGE

Makes it a crime, under certain conditions, to intentionally disseminate a synthetic intimate image; as under existing law, it is a class A misdemeanor if the image is disseminated to one person and a class D felony if it is disseminated to more than one through certain electronic means

§ 11 — OFFICE OF WORKFORCE STRATEGY

Requires the chief workforce officer to (1) incorporate AI into workforce training programs, (2) support the promotion of access to broadband internet access, and (3) coordinate an application to the federal government to seek federal funding for scholarships and apprenticeships that lead to a bachelor's degree in certain engineering fields

§§ 12 & 13 — INFORMATION AND TELECOMMUNICATION SYSTEMS STRATEGIC PLAN

Expands the information and telecommunication systems strategic plan to include any current or planned use of generative AI and potential opportunities and associated challenges

§ 14 — CONNECTICUT AI ACADEMY

Requires BOR to (1) establish a "Connecticut Citizens Academy" to offer online courses on AI and its responsible use and (2) award certificates and badges for completion

§ 15 — CT AI SYMPOSIUM

Requires DECD, by December 31, 2025, to conduct a "CT AI Symposium"

§ 16 — DECD AI POINT OF CONTACT

Requires the DECD commissioner to designate an employee as the primary point of contact for economic development in the AI field

§ 17 — WORKING GROUP

Establishes a working group to engage stakeholders and experts to make recommendations on certain AI-related issues

§§ 18 & 19 — TECHNOLOGY TALENT AND INNOVATION FUND

Repurposes the "Technology Talent Advisory Committee" to develop programs to expand the technology talent pipeline in the state in the fields of AI and quantum computing

BACKGROUND

SUMMARY

This bill establishes a framework for regulating artificial intelligence and includes other AI-related provisions, described in the section-by-section analysis below.

*Senate Amendment "A":

1. redefines certain terms, including "high-risk AI system" and "intentional and substantial modification";

2. delays various effective dates;

3. removes from the underlying bill (a) enforcement provisions for the Department of Consumer Protection (DCP) and Commission on Human Rights and Opportunities (CHRO), (b) a health care study provision, (c) authorization for DCP to adopt regulations on developer documentation, (d) violation reporting and notice requirements, and (e) a Department of Public Health study on AI in health care;

4. adds provisions on (a) adverse decision appeals, (b) consumer notice requirements, (c) AI trainings for state agency employees, and (d) a broadband access outreach program;

5. modifies provisions on (a) developer disclosures, (b) deeming systems in compliance, and (c) penalties for deceptive media distribution before an election;

6. adds the CHRO executive director to the AI Advisory Council;

7. modifies the provision on unlawful dissemination of an intimate image by including it in an existing crime; and

8. makes various minor, technical, and conforming changes.

*Senate Amendment "B" replaces Senate Amendment "A" and:

1. redefines certain terms, including "high-risk AI system" and "substantial factor";

2. further delays various effective dates;

3. removes the provisions on general-purpose AI model developer requirements;

4. exempts certain AI developers with fewer than 50 employees from certain requirements (e.g., impact assessments);

5. expands exemptions for systems that comply with federal agency standards or are working under a federal contract;

6. deems certain banks and credit unions in compliance under certain conditions;

7. adds provisions on the Connecticut Academy of Science and Engineering (CASE) liaisons, information and telecommunication systems strategic plan, and technology talent and innovation fund;

8. eliminates the advisory council provision and replaces it with a working group;

9. eliminates the (a) provisions requiring various collaborations, certificate programs, pilot studies, and programs and (b) provision on remote patient monitoring;

10. modifies the requirements for the Office of Workforce Strategy and elections and deceptive AI media; and

11. makes various minor, technical, and conforming changes.

EFFECTIVE DATE: July 1, 2025, except when otherwise noted below.

§§ 1-3 — REASONABLE CARE

Requires each developer and deployer of a high-risk AI system, beginning February 1, 2026, to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination

Beginning February 1, 2026, the bill requires each developer and deployer of a high-risk AI system to use reasonable care to protect consumers (i.e., Connecticut residents) from any known or reasonably foreseeable risks of algorithmic discrimination. An AI system is any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

Under the bill, a "developer" is any person (i.e., individual, association, corporation, limited liability company, partnership, trust, or other legal entity) doing business in the state who develops or intentionally and substantially modifies:

1. a general-purpose AI model (i.e., any form of AI system that displays significant generality, is capable of competently performing a wide range of distinct tasks, and can be integrated into a variety of downstream applications or systems, but not an AI model used for developing, prototyping, and researching activities before the model is released to the market); or

2. a high-risk AI system.

A high-risk AI system is a system that when deployed, makes, or is a substantial factor in making, a consequential decision. It does not include any:

1. AI system intended to perform a narrow procedural task; detect a decision-making pattern or deviation from a preexisting pattern unless the AI is intended to influence or replace a previously completed assessment by an individual without proper human review;

2. anti-fraud technology that does not use facial recognition technology or any anti-malware, anti-virus, calculator, cybersecurity, database, data storage, firewall, internet domain registration, internet-web-site loading, networking, robocall-filtering, spam-filtering, spellchecking, spreadsheet, web-

caching, web-hosting, or similar technology unless the technology, when deployed, makes, or is a substantial factor in making, a consequential decision; or

3. technology that communicates in natural language to give users information, make referrals or recommendations, and answers questions, and is subject to an accepted use policy which prohibits generating discriminatory or harmful content.

Under the bill, a "consequential decision" is any decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of, any (1) criminal case assessment, sentencing or plea agreement analysis, or a pardon, parole, probation, or release decision; (2) education enrollment or opportunity; (3) employment or employment opportunity; (4) financial or lending service; (5) essential government service; (6) health care service; or (7) housing, insurance, or legal service.

An "intentional and substantial modification" is any deliberate change made to:

1. an AI system that results in a new reasonably foreseeable risk of algorithmic discrimination or

2. a general-purpose AI model that affects the model's compliance, materially changes the model's purpose, or results in any new reasonably foreseeable risk of algorithmic discrimination.

It does not include any change made to, or the performance of, a high-risk AI system, if the system continues to learn after it is offered, sold, leased, licensed, given, or otherwise made available to a deployer, or deployed, and (1) the change is made to the system because of any AI learning (see above); (2) was predetermined by the deployer or the deployer's third party contractor, when the deployer or contractor completed the initial impact assessment for the system; and (3) is included in the system's technical documentation.

"Algorithmic discrimination" is any condition in which using an AI

system materially increases the risk of an unlawful differential treatment or impact that disfavors an individual or group of individuals based on their actual or perceived age, color, disability, ethnicity, genetic information, limited English language proficiency, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under federal or Connecticut law.

It does not include any:

1. offer, license, or use of a high-risk AI system by a developer or deployer solely for (a) self-testing to identify, mitigate, or prevent discrimination or ensure compliance with state and federal law, or (b) expanding an applicant, customer, or participant pool to increase diversity or redress historic discrimination, or

2. act or omission by or on behalf of a club or other establishment that is not open to the public as outlined in the federal Civil Rights Act of 1964 (42 U.S.C. § 2000a(e)).

Enforcement

Under the bill, in any enforcement action the attorney general brings after February 1, 2026, there is a rebuttable presumption that a developer or deployer used reasonable care if the developer or deployer complied with the relevant requirements under the bill.

§ 2 — DEVELOPERS

Generally requires, beginning February 1, 2026, that any developer making a high-risk AI system available to a deployer give the deployer a general statement describing the system's intended uses and certain documentation that describes the system, other information related to risk mitigation, and a statement summary; allows the attorney general to inspect these documents

General Statement of Intended Uses and Other Documentation

The bill generally requires, beginning February 1, 2026, any high-risk AI system developer to make available to a deployer or other developer a general statement describing the system's intended uses and certain documentation. The required documentation must disclose:

1. high level summaries of the data types used to train the system;

2. known or reasonably foreseeable limitations to the system, including risks of algorithmic discrimination arising from the intended uses; and

3. the system's purpose and intended benefits and uses.

The documentation must also describe:

1. how the system was evaluated for performance before it was offered, sold, leased, licensed, given, or otherwise made available to the deployer;

2. the governance measures used to cover the training datasets and the measures used to examine the suitability of the data sources, possible biases, and appropriate mitigation;

3. the system's intended outputs;

4. the measures the developer took to mitigate any known or reasonably foreseeable risks of algorithmic discrimination that may arise from the system being deployed; and

5. a description of how an individual should use or monitor the system when the system is used to make, or is a substantial factor in making, a consequential decision.

The developer must also give the deployer documentation that is reasonably necessary to help the deployer understand the system's outputs and monitor the system's performance for any risk of algorithmic discrimination.

Risk Mitigation

On and after February 1, 2026, the bill requires, among other things, a high-risk AI systems developer that offers, sells, leases, licenses, gives, or otherwise makes available to a deployer a high-risk AI system to give the deployer, to the extent feasible, the documentation and information needed for the deployer or its third-party contractor to complete an impact assessment the bill requires (see § 3 below). The developer must provide the documentation and information to the deployer through

artifacts such as model cards, dataset cards, or other impact assessments.

A developer that also serves as a deployer for these systems does not have to generate this documentation unless the system is provided to an unaffiliated entity acting as a deployer.

Statement Summary

Beginning on that same date, developers must make available, in a clear and readily available way, a statement summarizing certain aspects of the high-risk AI system. They must make the summary available for public inspection on their website or in a public use case inventory. The summary statement must include:

1. the types of high-risk AI systems the developer (a) has developed or intentionally and substantially modified and (b) currently makes available to deployers and

2. how the developer manages known or reasonably foreseeable risks of algorithmic discrimination arising from development or intentional and substantial modification of these types of high-risk AI systems described above.

The bill requires each developer to update the statement (1) as needed to ensure that it remains accurate and (2) within 90 days after the developer intentionally and substantially modifies any high-risk AI system.

Trade Secrets

The bill specifies that the developer provisions above should not be construed to require a developer to disclose any trade secret or other confidential or proprietary information.

Under the bill, a "trade secret" is information, including a formula, pattern, compilation, program, device, method, technique, process, drawing, cost data, or customer list, that (1) derives actual or potential independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other individuals

who can obtain economic value from its disclosure or use and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Disclosure

The bill allows the attorney general, beginning February 1, 2026, to require developers to disclose to him, through written demand, among other ways, any statement or documentation described above if it is relevant to an investigation he conducts. The attorney general may evaluate the statement or documentation to ensure compliance with these provisions. The bill exempts from disclosure under the Freedom of Information Act (FOIA) any statement or documentation that includes proprietary information or trade secrets. A developer may designate these statements or documentation as having proprietary information or trade secrets. To the extent any information in a disclosed document includes information subject to attorney-client privilege or work product protection, the act specifies that a disclosure does not constitute a waiver of the privilege or protection.

§ 3 — DEPLOYERS

Generally requires deployers, beginning February 1, 2026, to (1) implement a risk management policy and program before deploying high-risk AI systems; (2) complete an impact assessment on the system before deploying or after any intentional and substantial modification of it; (3) review each deployed system at least annually to ensure the system is not causing algorithmic discrimination; and (4) disclose risk management policies, impact assessments, and records to the attorney general if relevant to an investigation

Risk Management Policy and Program

The bill generally requires deployers, beginning on February 1, 2026, to implement and maintain a risk management policy and program to govern the deployer's deployment of a high-risk AI system. The policy and program must specify and incorporate the principles, processes, and personnel the deployer uses to identify, document, and mitigate any known or reasonably foreseeable risks of algorithmic discrimination. The risk management program must be an iterative process that is planned, implemented, and regularly and systematically reviewed and updated over the system's lifecycle. Each policy and program implemented and maintained must be reasonable, considering the:

1. guidance and standards set by the latest version of the National Institute of Standards and Technology's "Artificial Intelligence Risk Management Framework" (ISO/IEC 42001), or another nationally or internationally recognized risk management framework for AI systems;

2. deployer's size and complexity;

3. nature and scope of the high-risk AI system the deployer deployed, including its intended uses; and

4. sensitivity and volume of data processed in connection with the systems the deployer deployed.

The bill allows a risk management policy and program to cover multiple high-risk AI systems deployed by the same deployer.

Impact Assessment

The bill requires a high-risk AI system deployer or its third-party contractor to, at least annually and by February 1, 2026, complete an impact statement for a deployed high-risk AI system. Additionally, on or after the same date, they must complete an impact assessment on the system within 90 days after any intentional and substantial modification is made available.

Each impact assessment must at least include, to the extent reasonably known by, or available to, the deployer:

1. a statement by the deployer disclosing the system's purpose, intended use cases, and deployment context and benefits;

2. an analysis of whether deploying the system poses any known or reasonably foreseeable risks of algorithmic discrimination and, if so, the nature of the discrimination and steps taken to eliminate the risks;

3. a description of the (a) data categories the system processes as inputs and (b) outputs the system produces;

4. if the deployer used data to customize the system, an overview of the data categories the deployer used to customize the system;

5. any metrics used to evaluate the system's performance and known limitations;

6. a description of any transparency measures taken on the system, including any measures taken to disclose to a consumer that the system is in use when it is in use; and

7. a description of the post-deployment monitoring and user safeguards provided on the system, including the oversight process the deployer established to address issues from deploying the system.

Additional Statement. In addition to the impact assessment after an intentional and substantial modification to the system, the bill requires a statement disclosing the extent to which the system was used in a manner that was consistent with, or varied from, the developer's intended uses of the system.

Single Assessment. The bill allows a single assessment to address a comparable set of systems a deployer deploys. If a deployer or its third-party contractor completes an assessment to comply with another applicable law or regulation, that assessment is deemed to satisfy the assessment requirements if the assessment is reasonably similar in scope and effect as the assessment would have been if completed under this provision.

Completed Assessments. A deployer must maintain the most recently completed assessment, any prior ones, and all records on each assessment for at least three years after the final deployment of the system.

Annual Review

The bill requires a deployer, or its third-party contractor, to review, at least annually, each system the deployer deployed to ensure it is not causing algorithmic discrimination.

Notification

Beginning February 1, 2026, and by the time a deployer deploys a high-risk AI system to make, or be a substantial factor in making, a consequential decision concerning a consumer, the deployer must (1) notify the consumer that the deployer has deployed a system to make, or be a substantial factor in making, the consequential decision and (2) give the consumer the deployer's contact information, a statement disclosing the system's purpose and nature of the consequential decision, and instructions on how to access the statement available for public inspection (see below).

If the deployer is also a controller under the data privacy law (those that determine the purpose and means of processing personal data), then the deployer must also (1) disclose the consumer's right to opt-out of having his or her personal data processed for profiling to further solely automated decisions that produce legal or similarly significant effects and (2) give the consumer an opportunity to submit notice that the consumer is opting out. If the request is verifiable, the deployer must respond to the request without imposing any cost to the consumer, without undue delay but within 45 days after the deployer receives the request. If it is not feasible due to technical limitations, the deployer must notify the consumer that it cannot feasibly comply and disclose the technical limitation.

The deployer must generally provide this notice, statement, contact information, description, and statements related to adverse consequential decisions (see below) directly to the consumer; in plain language; in all languages the deployer, in the ordinary course of such deployer's business, provides contracts, disclaimers, sale announcements, and other information to consumers; and in a format accessible to consumers with disabilities. If the deployer is unable to provide this information directly, the deployer must do it in a manner reasonably calculated to ensure the consumer receives it.

Adverse Consequential Decisions

Beginning January 1, 2026, the bill requires a deployer that has deployed a system to make, or as a substantial factor in making, a

consequential decision concerning a consumer, to give the consumer certain notices and opportunities to correct incorrect information or appeal adverse consequential decisions.

In these instances, the deployer must give the consumer a statement disclosing the principal reason or reasons for the consequential decision, including the:

1. degree to which, and manner in which, the system contributed to the consequential decision;

2. data that the system processed in making the consequential decision; and

3. data source or sources.

The deployer must also allow the consumer an opportunity to:

1. correct any incorrect personal data that the system processed in making, or as a substantial factor in making, the consequential decision and

2. appeal any adverse consequential decision from the system deployment, with a human review, if technically feasible, unless doing so is not in the consumer's best interest (e.g., when delay might pose a risk to a consumer's life or safety).

Public Inspection

The bill requires each deployer to make available, in a way that is clear and readily available for public inspection, a statement summarizing:

1. the types of high-risk artificial intelligence systems that the deployer currently deploys,

2. how the deployer manages any known or reasonably foreseeable risks of algorithmic discrimination that may arise from deploying each system, and

3. in detail, the nature, source, and extent of information the deployer collects and uses.

A deployer must also periodically update this statement.

Exemption

The bill exempts deployers from its risk management, impact assessments, annual review, and public inspection requirements if, at the time the deployer deploys a system and at all times while the system is deployed, the:

1. deployer (a) employs fewer than 50 full time equivalent employees and (b) does not use the deployer's own data to train the system;

2. system (a) is used for the intended uses disclosed to the deployer and (b) if it continues learning, is based on data derived from sources other than the deployer's own data; and

3. deployer makes available to consumers any impact assessment that (a) the developer has completed and given to the deployer and (b) includes a statement, analysis, description, overview, and metrics that are substantially similar to those required by the bill for impact assessments.

Trade Secrets

The bill specifies that the deployer provisions above should not be construed to require a deployer to disclose any trade secret or other confidential or proprietary information.

Disclosure

Substantially similar to the developer disclosure provision in § 2, the bill allows the attorney general, beginning February 1, 2026, to require deployers and their third-party contractors to disclose any risk management policy, impact assessment, or record if it is relevant to an investigation. The attorney general may evaluate these items to ensure compliance with these provisions. Under the bill, these documents are exempt from FOIA disclosure if they contain any proprietary

information or trade secret as designated by a deployer or its third-party contractor, and a disclosure does not constitute a waiver of the attorney-client privilege or work product protection.

§ 4 — PUBLIC DISCLOSURE REQUIREMENTS

Generally requires, beginning February 1, 2026, anyone doing business in Connecticut who deploys an AI system that interacts with consumers to ensure it is disclosed to each consumer the system interacts with that the consumer is interacting with an AI system

Beginning February 1, 2026, the bill generally requires anyone doing business in the state, including each deployer that deploys, offers, sells, leases, licenses, gives, or otherwise makes available, as applicable, an AI system that is intended to interact with consumers, to ensure that it is disclosed to each consumer who interacts with the system that the consumer is interacting with an AI system.

This disclosure is not required when a reasonable person would deem it obvious that he or she is interacting with an AI system.

§ 5 — SYNTHETIC DIGITAL CONTENT

Generally requires, beginning February 1, 2026, an AI system developer that generates or manipulates synthetic digital content to include certain labels or technical solutions

Developer Labeling and Technical Standards

Beginning February 1, 2026, the bill generally requires developers of AI systems that generate or manipulate synthetic digital content to include certain labels and ensure their technical solutions are effective, among other things.

Under the bill, "synthetic digital content" is any digital content, including any audio, image, text, or video, that is produced or manipulated by an AI system, including a general-purpose AI model.

The AI system developer must ensure the AI system outputs are marked and detectable as synthetic digital content (1) by the time the consumer, who did not create the outputs, first interacts with, or is exposed to, the outputs and (2) in a way that is detectable by consumers and complies with any applicable accessibility requirements. As technically feasible and in a way that is consistent with any nationally or internationally recognized technical standards, the developer must

ensure its technical solutions are effective, interoperable, robust, and reliable, considering the specificities and limitations of the different types of synthetic digital content, the implementation costs, and the generally acknowledged state-of-the-art.

Exemptions. For synthetic digital content that is in an audio, image, or video format and is part of an evidently artistic, creative, satirical, fictional analogous work or program, the required disclosure may be limited to a disclosure that does not hinder the display or enjoyment of the work or program.

Additionally, no disclosure is required if the synthetic digital content:

1. consists exclusively of text,
2. is published to inform the public on matters of public interest,
3. has undergone a process of human review or editorial control,
4. is unlikely to mislead a reasonable person consuming the content, or
5. is subject to control by a person who holds editorial responsibility for publishing the content.

The disclosure requirements also do not apply to the extent any AI system is used to perform an assistive function for standard editing; does not substantially alter the input data the developer provides or its semantics; or is used to detect, prevent, investigate, or prosecute any crime when authorized by law.

§ 6 — ABILITY TO COMPLY WITH STATE OR FEDERAL LAWS OR TAKE CERTAIN OTHER ACTIONS

Specifies that the bill's requirements do not restrict a developer's or deployer's ability to take certain actions (e.g., comply with federal and state law, cooperate with law enforcement, and engage in research)

Compliance and Other Actions

The bill specifies that nothing in its provisions should be construed to restrict a developer's, deployer's, or other person's ability to:

1. comply with federal, state, or municipal ordinances or regulations, or a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other governmental authorities;

2. cooperate with law enforcement agencies concerning conduct or activity that the developer or deployer reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations;

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

4. take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or a person;

5. by any means other than facial recognition technology, 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 these actions;

6. engage in public- or peer-reviewed scientific or statistical research in the public interest that (a) follows applicable ethics and privacy laws and (b) is conducted under the federal policy for protecting human subjects (45 C.F.R. Part 46) and relevant requirements under the federal Food and Drug Administration (FDA);

7. conduct any research, testing, and development activities on any AI system or model, other than testing under real world conditions, before it is placed on the market, deployed, or put into service, as applicable;

8. effectuate a product recall;

9. identify and repair technical errors that impair functionality; or

10. assist another developer, deployer, or other person with any obligations imposed by the bill.

Constitutional Rights and Obligations

The bill states that its provisions are not to be construed to impose an obligation on a developer, deployer, or other person that adversely affects the rights and freedoms of any person, including rights to free speech or freedom of the press guaranteed under the First Amendment of the U.S. Constitution or rights under the state law protecting news media from compelled disclosure of information (CGS § 52-146t).

Federal Approvals, Research, and Work

The bill exempts from its requirements any developer, deployer, or other person who develops, deploys, puts into service, or intentionally and substantially modifies a high-risk AI system that:

1. has been approved, authorized, certified, cleared, or granted by a federal agency, such as the FDA or the Federal Aviation Administration (FAA), acting within their agency authority, or in compliance with federal agency standards, including the federal Office of the National Coordinator for Health Information Technology standards; or

2. conducts any research to support an application for approval or certification from any federal agency, including the FAA, FDA, or Federal Communications Commission, or otherwise subject to agency review;

3. performs work under, or in connection with, a contract with the U.S. departments of Commerce or Defense or NASA, unless the developer, deployer, or other person is performing the work on a high-risk AI system that is used to make, or as a substantial factor in making, a decision concerning employment or housing; or

4. is a covered entity under the Health Insurance Portability and Accountability Act (HIPAA) and is providing health care recommendations that (a) are AI-generated, (b) require a health

care provider to take action to implement the recommendations, and (c) are not considered to be high-risk.

The bill specifies that its provisions should not be construed to apply to any AI system that is acquired by or for the federal government or any federal agency or department, including the U.S. departments of Commerce or Defense or NASA, unless the system is a high-risk AI system that is used to make, or as a substantial factor in making, a decision concerning employment or housing.

Insurers

Under the bill, any insurer, fraternal benefit society, or health carrier is deemed in full compliance with the bill's provisions if it has implemented and maintains a written AI systems program under all the requirements the Insurance Commissioner establishes.

Banking Entities

The bill deems certain banking entities to be in full compliance with the bill's requirements if the entity is subject to examination by a state or federal prudential regulator under any published guidance or regulations that apply to using high-risk AI systems that meet certain standards. The guidance or regulations must impose requirements that are substantially similar to the bill's requirements and require the banking entity to:

1. regularly audit its use of high-risk AI systems for compliance with applicable state and federal anti-discrimination laws and regulations and

2. mitigate any algorithmic discrimination the system causes or that is reasonably foreseeable because of system use.

This exemption applies to banks; out-of-state banks; Connecticut, out-of-state, or federal credit unions; or any affiliate or subsidiary.

Under the bill, if a developer, deployer, or other person engages in an exempted action, it bears the burden of demonstrating that the action qualifies for the exemption.

§ 7 — ATTORNEY GENERAL ENFORCEMENT

Gives the attorney general exclusive authority to enforce the AI provisions listed above; requires a one-year grace period to allow violators an opportunity to cure violations; provides certain affirmative defenses; and deems violations CUTPA violations, but does not provide a private right of action

Under the bill, the attorney general has exclusive authority to enforce the AI provisions above.

The bill establishes a grace period from February 1, 2026, to January 31, 2027, during which the attorney general must give violators an opportunity to cure any violations. Beginning February 1, 2027, the bill gives the attorney general discretion over whether to provide an opportunity to correct an alleged violation.

The bill specifies that none of its provisions should be construed as providing the basis for, or be subject to, a private right of action for violations under the act or any other law.

Under the bill, any violation of the bill's requirements is a Connecticut Unfair Trade Practices Act (CUTPA) violation, except for ones occurring during the grace period, those the attorney general allows a violator to cure, or those with an affirmative defense. Additionally, CUTPA's private right of action and class action provisions do not apply to violations.

Notice of and Opportunity to Correct Violations

The bill generally requires the attorney general to allow a grace period to give violators an opportunity to cure a violation between February 1, 2026, to January 31, 2027. The bill requires the attorney general, before initiating any action for a violation, to issue a notice of violation to the deployer, developer, or other person if he determines a cure is possible. If the deployer, developer, or other person fails to cure the violation within 60 days after receiving notice, the attorney general may bring an action to enforce.

Violations After February 1, 2027. Beginning on February 1, 2027, the attorney general may, in determining whether to give a deployer, developer, or other person the opportunity to cure an alleged

discriminatory practice, consider:

1. the number of violations;

2. the deployer's, developer's, or other person's size and complexity and the nature and extent of its business;

3. the substantial likelihood of injury to the public;

4. the safety of individuals or property; and

5. whether the alleged violation was likely caused by human or technical error.

Affirmative Defenses

Under the bill, in any attorney general action, it is an affirmative defense that the developer, deployer, or other person:

1. discovered a violation (a) due to the feedback they encourage deployers or users to provide; (b) through adversarial testing or red-teaming, as defined or used by the National Institute of Standards and Technology; or (c) through an internal review process;

2. within 60 days after discovering the violation, cured it and notified the attorney general, in a form and manner he prescribes, that the violation has been cured with evidence that any harm the violation caused has been mitigated; and

3. otherwise complies with the latest version of the "Artificial Intelligence Risk Management Framework" that the National Institute of Standards and Technology publishes or another nationally or internationally recognized risk management framework for AI systems.

Generally, "adversarial testing" is a method for systematically evaluating a machine learning model with the intent of learning how it behaves when provided with malicious or inadvertently harmful input. A "Red Team" is a group of people authorized and organized to

simulate a potential adversary's attack or exploitation capabilities against a security posture. The Red Team's objective is to improve cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

The developer, deployer or other person bears the burden of demonstrating to the attorney general that the requirements for these affirmative defenses have been satisfied.

Under the bill, the attorney general must not initiate any enforcement action unless he has consulted with the CHRO executive director to determine whether any complaint has been filed with the commission based on the same act or omission. The attorney general cannot initiate an enforcement action unless the complaint has been finally adjudicated or resolved.

The bill specifies that it should not be construed to preempt or affect any right, claim, remedy, presumption, or defense available under the law or equity. Any rebuttable presumption or affirmative defense the bill establishes only applies to an attorney general enforcement action and does not apply to any of the legal actions stated above.

The bill also requires the attorney general to post on the attorney general's website information on how to properly file a complaint with CHRO.

§ 8 — CONNECTICUT ACADEMY OF SCIENCE AND ENGINEERING (CASE) LIAISONS

Allows legislative leaders to request CASE members to serve as a liaison between the academy and state government; requires liaisons to serve certain purposes, such as designing tools to determine compliance with the bill's requirements and evaluating the adoption of AI systems by businesses

The bill allows each legislative leader (House speaker, Senate president pro tempore, and House and Senate minority leaders) to request that the Connecticut Academy of Science and Engineering (CASE) designate a member to serve as the leader's liaison with the academy, the Office of the Attorney General, and the Department of Economic and Community Development (DECD). The liaison's purpose

is to:

1. design a tool to (a) allow anyone to determine whether they are in compliance with the bill's requirements and (b) help a deployer or its third-party contractor complete an impact assessment;

2. meet with relevant stakeholders to form a plan to use UConn School of Law's Intellectual Property and Entrepreneurship Law Clinic to assist small businesses and startups in their efforts to comply with the bill's provisions;

3. make recommendations for establishing a framework to provide a controlled and supervised environment where AI systems may be tested, which must at least include recommendations on establishing (a) an office to oversee the framework and environment and (b) a program that would enable consultations between the state, businesses, and other stakeholders on the framework and environment;

4. evaluate (a) the adoption of AI systems by businesses; (b) the challenges posed to, and needs of, businesses in adopting these systems, and understanding laws and regulations on these systems; and (c) how businesses that use these systems hire employees with necessary skills for them;

5. create a plan for the state to provide high-performance computing services to businesses and researchers in Connecticut;

6. evaluate the benefits of creating a state-wide research collaborative among health care providers to enable the development of advanced analytics, ethical, and trustworthy AI systems, and hands-on workforce education while using methods that protect patient privacy; and

7. evaluate and make recommendations on (a) the establishment of testbeds to support safeguards and systems to prevent misusing AI systems; (b) risk assessments for misusing AI systems; (c)

evaluation strategies for AI systems; and (d) the development, testing, and evaluation of resources to support state oversight of AI systems.

The bill prohibits any CASE-designated member from being deemed a state employee or receiving any compensation from the state for performing his or her duties under this provision.

§ 9 — ELECTIONS AND DECEPTIVE AI MEDIA

Generally makes it a crime for a person (e.g., individual or entity) to knowingly distribute a communication with deceptive synthetic media within 90 days before an election or primary

This bill generally makes it a crime for a person to (1) distribute a communication with deceptive synthetic media or (2) enter into an agreement to distribute it. Under the bill, a "person" is an individual, committee, firm, partnership, organization, association, syndicate, company trust, corporation, limited liability company, or any other legal entity, but not the state or any of its political or administrative subdivisions.

Specifically, the bill prohibits this if it takes place within 90 days before an election or primary and:

1. the person knows, or should reasonably know, it is deceptive synthetic media or if the individual depicted is a public official or figure, acts with reckless disregard as to whether the image, audio, or video is deceptive synthetic media;

2. it is distributed without the depicted individual's consent; and

3. the person recklessly disregards the risk that the distribution will injure a candidate or influence the election or primary results.

However, the bill exempts certain deceptive synthetic media that is distributed if it has a disclaimer as required by the bill. Further, news organizations and other similar entities may be exempt from criminal and civil liability if the distribution is part of bona fide news coverage on the deceptive communication.

The bill also allows the attorney general and certain people to bring a civil action against someone who violates the bill's provisions and subjects violators to criminal penalties ranging from a class C misdemeanor to a class D felony, depending on the circumstances.

EFFECTIVE DATE: July 1, 2024

Deceptive Synthetic Media

Under the bill, "deceptive synthetic media" is any image, audio, or video of an individual, and any representation of his or her appearance, speech, or conduct that is substantially derived from it, which (1) a reasonable person would believe depicts the individual's appearance, speech, or conduct when the individual did not do so and (2) was generated, in whole or in part, by using artificial intelligence or other technology.

Disclaimer

Under the bill, deceptive synthetic media may be distributed lawfully within the 90-day period if it contains a disclaimer using specific words, or using substantially the same words, as required by the bill. The disclaimer varies depending on the type of media (i.e., image, audio, or video).

Image Disclaimer. Under the bill, the image must contain a disclaimer stating either "This communication contains an image that has been manipulated" or "This image has been manipulated," as applicable. Additionally, the disclaimer must:

1. appear in text clearly visible to and easily readable by the average viewer;

2. be in text at least the same size as the largest font used for any other text in the communication; and

3. contain a citation to the original source of the unedited or unmanipulated version of the image, if the media was generated by editing or manipulating an existing image.

Audio Disclaimer. The audio must contain a disclaimer stating, "This communication contains audio that has been manipulated." Additionally, the disclaimer must:

1. be read in a clearly spoken manner;

2. be in a pitch that can be heard by the average listener;

3. be read in the same language as the rest of the media as well as any other language the person would reasonably expect the listener to speak or understand; and

4. contain a citation to the original source of the unedited or unmanipulated version of the audio, if the media was generated by editing or manipulating existing audio.

The disclaimer must be read at the beginning and end of the communication. If the communication is greater than one minute, it must be read during the audio at least every 30 seconds.

Video Disclaimer. The video must contain a disclaimer stating, "This communication contains video that has been manipulated." Additionally, the disclaimer must:

1. appear throughout the entire video in text clearly visible to and easily readable by the average viewer;

2. be in text at least the same size as the largest font used for any other text in the communication;

3. be in the same language as the rest of the media as well as any other language the person would reasonably expect the listener to speak or understand; and

4. contain a citation to the original source of the unedited or unmanipulated version of the video, if the media was generated by editing or manipulating existing video.

Exempt Entities

The bill's provisions do not apply, under certain conditions, to a radio or television station, a website, streaming or other digital broadcast service provider, or a regularly published newspaper, magazine, or online periodical of general circulation.

Radio or television stations (including broadcast, cable, and satellite) may broadcast deceptive synthetic media if it is part of a bona fide newscast, news interview, news documentary, or other on-the-spot coverage of bona fide news events.

The broadcast must either retain the disclaimer required by the bill or add one if the original communication did not contain one, except for on-the-spot coverage. Additionally, a broadcast must clearly state in its content that the communication contains deceptive synthetic media, except for on-the-spot coverage of a communication that the person does not have reason to believe contains deceptive synthetic media.

Websites or regular periodicals may publish this media if (1) it is part of their routine news coverage and commentary of general interest, (2) they retain the disclaimer required by the bill or add one if not present, and (3) they clearly state in their content that the communication contains deceptive synthetic media.

The bill requires anyone who purchase political advertising space on one of the broadcast entities above, to file an affirmation with the State Elections Enforcement Commission, sworn under the penalties of false statement, that the communication does not contain any deceptive synthetic media. The person must give a copy of the affirmation to the entity, which must preserve the copy for four years from when the communication was last broadcast.

Penalties

Criminal. At a minimum, a violation can result in a class C misdemeanor, which carries a maximum penalty of incarceration of three months, a $500 fine, or both. For violations committed with the intent to cause violence or bodily harm or distributed to an audience of more than 10,000 individuals, the penalty is increased to a class A

misdemeanor (up to 364 days imprisonment, a fine of $2,000, or both). The penalty may also be increased to a class D felony (up to five years imprisonment, a $5,000 fine, or both) for a subsequent conviction within five years.

These criminal penalties are in addition to any injunctive or equitable relief or special damages pursued in a civil action.

Civil. The bill also allows (1) the attorney general, (2) an individual depicted in the deceptive media, or (3) a candidate injured or likely to be injured by the media's distribution, to seek a permanent injunction or other equitable relief against a person violating, or that will imminently violate, the bill. The plaintiff must prove their claim by clear and convincing evidence.

Plaintiffs, other than the attorney general, may seek general or special damages due to the distribution and must be awarded attorney's fees and costs if they prevail.

Satire

The bill specifies that this prohibition does not apply to any:

1. image, audio, or video of an individual, or any representation of an individual's appearance, speech, or conduct that is substantially derived from an image, audio, or video, that is considered parody or satire, as long as a reasonable person would not believe that the individual in fact appeared or engaged in speech or conduct as depicted, or

2. political advertising or campaign communication that the law requires to be distributed, including under the federal "equal time" rule and related regulations (47 U.S.C. § 315).

§ 10 — UNLAWFUL DISSEMINATION OF AN INTIMATE IMAGE

Makes it a crime, under certain conditions, to intentionally disseminate a synthetic intimate image; as under existing law, it is a class A misdemeanor if the image is disseminated to one person and a class D felony if it is disseminated to more than one through certain electronic means

The bill makes it a crime, under certain conditions, to intentionally

disseminate a synthetic intimate image. The bill does so by specifying that the dissemination of these images is included within the existing crime of unlawful dissemination of an intimate image. Under the bill, a "synthetic image" is any photograph, film, videotape, or other image that (1) is not wholly recorded by a camera; (2) is either partially or wholly generated by a computer system; and (3) depicts, and is virtually indistinguishable from an actual representation of, an identifiable person.

Under current law, someone is guilty of this crime when the person intentionally disseminates an intimate image (including video) without the other person's consent, knowing that the other person believed the image would not be disseminated, and the other person suffers harm because of this. The bill eliminates the requirement that the person believed the image would not be disseminated.

As under existing law, this crime applies to images of a person in certain degrees of nudity or engaged in sexual intercourse. It does not apply in certain circumstances, such as if the image resulted from voluntary exposure in public.

By law, this crime is a (1) class A misdemeanor (punishable by up to 364 days in prison, a fine of up to $2,000, or both), or (2) class D felony (punishable by up to five years in prison, a fine of up to $5,000, or both) if the unlawful distribution is to multiple people by means of an interactive computer service, an information service, or a telecommunications service.

EFFECTIVE DATE: October 1, 2024

§ 11 — OFFICE OF WORKFORCE STRATEGY

Requires the chief workforce officer to (1) incorporate AI into workforce training programs, (2) support the promotion of access to broadband internet access, and (3) coordinate an application to the federal government to seek federal funding for scholarships and apprenticeships that lead to a bachelor's degree in certain engineering fields

By law, the Office of Workforce Strategy is led by the chief workforce officer, who is the principal advisor to the governor on workforce development policy, strategy, and coordination. The chief workforce

officer must also have knowledge about publicly funded workforce training programs and have the training and experience to perform certain statutory duties. The bill also requires her to:

1. incorporate digital literacy training into workforce training programs, including AI training in accordance with the digital equity principles, in consultation with higher education institutions, the regional workforce development boards, the Commission for Educational Technology, DECD, and other relevant state agencies;

2. support the promotion of access to broadband internet service through the workforce training programs and in accordance with digital equity principles and other state efforts to promote broadband internet service; and

3. coordinate, in consultation with DECD, higher education institutions, and industry, efforts to apply to the federal government under the CHIPS and Science Act of 2022 (P.L. 117-167) to obtain funding for a scholarship for diverse students seeking a bachelor's degree in electrical or mechanical engineering, and a registered apprenticeship that leads to a bachelor's degree in mechanical engineering.

EFFECTIVE DATE: July 1, 2024

§§ 12 & 13 — INFORMATION AND TELECOMMUNICATION SYSTEMS STRATEGIC PLAN

Expands the information and telecommunication systems strategic plan to include any current or planned use of generative AI and potential opportunities and associated challenges

The bill expands the state's information and telecommunication systems strategic plan to include any current or planned use of generative AI and potential opportunities and associated challenges, if these topics have been reviewed by a working group (see below; § 17) that includes representation from labor organizations and other internal and external stakeholders.

Existing law requires the Department of Administrative Services

(DAS) commissioner to develop, publish, and annually update this plan to facilitate development of a fully integrated statewide information services and telecommunication system to support state agencies. Among other things, the plan must include architecture guidelines and standards for these systems.

EFFECTIVE DATE: July 1, 2024

§ 14 — CONNECTICUT AI ACADEMY

Requires BOR to (1) establish a "Connecticut Citizens Academy" to offer online courses on AI and its responsible use and (2) award certificates and badges for completion

The bill requires the Board of Regents (BOR) to establish a "Connecticut AI Academy" to curate and offer online courses on AI and its responsible use. It must do this by December 31, 2025, on behalf of Charter Oak State College and in consultation with Connecticut independent institutions of higher education. BOR must also, in consultation with Charter Oak State College, develop certificates and badges to be awarded to individuals who successfully complete the courses. For this provision, AI means a machine-based system that (1) can make predictions, recommendations, or decisions based on a given set of human-defined objectives and (2) uses machine and human-based inputs to perceive real and virtual environments, abstract these perceptions into models through an automated analysis, and formulate options for information or action through model inference.

§ 15 — CT AI SYMPOSIUM

Requires DECD, by December 31, 2025, to conduct a "CT AI Symposium"

The bill requires DECD, by December 31, 2025, to partner with Connecticut higher education institutions and coordinate with industry to conduct a "CT AI Symposium" to foster collaboration between academia, government, and industry to promote the establishment and growth of AI businesses in the state.

§ 16 — DECD AI POINT OF CONTACT

Requires the DECD commissioner to designate an employee as the primary point of contact for economic development in the AI field

The bill requires the DECD commissioner to designate a department employee to serve as the primary point of contact for economic

development in the AI field.

EFFECTIVE DATE: July 1, 2024

§ 17 — WORKING GROUP

Establishes a working group to engage stakeholders and experts to make recommendations on certain AI-related issues

The bill establishes a working group to engage stakeholders and experts to make recommendations on:

1. the best practices to avoid the negative impacts, and to maximize the positive impacts, on services and state employees in connection with implementing new digital technologies and AI;

2. collecting reports, recommendations, and plans from state agencies considering AI implementation, and assessing these reports, recommendations, and plans against the best practices; and

3. any other matters the working group deems relevant for avoiding the negative impacts and maximizing the positive impacts.

The working group must also:

1. make recommendations on ways to create resources to help small businesses adopt AI to improve their efficiency and operations;

2. propose legislation to (a) regulate the use of general-purpose AI and (b) require social media platforms to provide a signal when they are displaying synthetic digital content;

3. propose other legislation on AI after reviewing other states' AI laws and regulations, and any proposed AI legislation or regulations;

4. develop an outreach plan to bridge the digital divide and provide workforce training to individuals who do not have high-speed internet access;

5. evaluate and make recommendations on (a) establishing testbeds to support safeguards and systems to prevent the AI misuse; (b) assessing risk for AI misuse; (c) evaluating AI strategies; and (d) developing, testing, and evaluating resources to support state oversight of AI;

6. review the protections for trade secrets and other proprietary information under existing state law and make recommendations on these protections;

7. study AI-related definitions, including the bill's definition of a high-risk AI system, and make recommendations on including language specifying that no AI system is considered to be a high-risk AI system if it does not pose a significant risk of harm to the health, safety, or fundamental rights of individuals, including, by not materially influencing the outcome of any decision-making;

8. review any current or planned use of generative AI and the potential opportunities and associated challenges with the purposes in the information and telecommunication systems strategic plan;

9. make recommendations for the establishment and membership of a permanent AI advisory council; and

10. make other recommendations on AI as the working group deems appropriate.

Voting Members

Under the bill, the working group has membership similar to the AI Working Group established in PA 23-16. The table below shows the working group's voting members. In addition, all voting members must have professional experience or academic qualifications in AI, automated systems, government policy, or another related field.

Table: Working Group Voting Member Appointment and Qualifications

Appointing Authority	*Member Qualifications*
House speaker	Representative of industries developing AI

Appointing Authority	*Member Qualifications*
Senate president pro tempore	Representative of industries using AI
House majority leader	Academic with a concentration in the study of technology and technology policy
Senate majority leader	Academic with a concentration in the study of government and public policy
House minority leader	Representative of an industry association for industries developing AI
Senate minority leader	Representative of an industry association for industries using AI
General Law Committee chairpersons (one appointment each)	Not specified
General Law Committee ranking members (one appointment each)	Representative of industry
Labor Committee chairpersons (one appointment each)	Representative of labor industry
Labor Committee ranking members (one appointment each)	Representative of small businesses
Governor (two appointments)	Two Connecticut Academy of Science and Engineering (CASE) members

The bill requires appointing authorities to make initial appointments within 30 days after the bill's passage and fill any vacancies. Any working group action must be taken by a majority vote of all voting members present, and no action may be taken unless at least 50% of voting members are present.

Nonvoting Ex-Officio Members

The working group also includes the General Law and Labor and Public Employees committees' chairpersons as nonvoting ex-officio members and the following nonvoting ex-officio members, or their designees:

1. attorney general;
2. state comptroller;
3. state treasurer;
4. DAS commissioner;

5. chief data officer;

6. Freedom of Information Commission executive director;

7. Commission on Women, Children, Seniors, Equity and Opportunity executive director;

8. chief court administrator; and

9. CASE executive director.

Chairpersons and Meetings

The bill makes the General Law Committee chairpersons and the CASE executive director the working group's chairpersons. They must schedule and hold the group's first meeting within 60 days after the bill's passage.

The bill requires the General Law Committee's administrative staff to serve as the working group's administrative staff.

Report

The bill requires the working group to submit a report on its findings and recommendations to the General Law Committee by February 1, 2025. The working group terminates on that date or when it submits the report, whichever is later.

EFFECTIVE DATE: Upon passage

§§ 18 & 19 — TECHNOLOGY TALENT AND INNOVATION FUND

Repurposes the "Technology Talent Advisory Committee" to develop programs to expand the technology talent pipeline in the state in the fields of AI and quantum computing

The bill repurposes the "Technology Talent Advisory Committee" within DECD and renames it the "Technology Talent and Innovation Fund Advisory Committee."

Under current law, the committee must (1) calculate certain statistics on the number of state residents in technology-related fields and (2) develop pilot programs for recruiting software developers and training state residents in software development and other topics.

The bill eliminates these requirements and instead requires the committee to develop programs to expand the state's technology talent pipeline, including in the fields of AI and quantum computing. It allows the committee to partner with higher education institutions and other nonprofit organizations in developing these programs.

By July 1, 2025, the bill requires the committee to partner with Connecticut higher education institutions and other training providers to develop programs in the AI field, including in areas such as prompt engineering (i.e., the process of guiding a generative AI system to generate a desired output), AI marketing for small businesses, and AI for small business operations.

As under existing law, the DECD commissioner determines the committee's size and appoints the members, which must at least include representatives of UConn, the Board of Regents for Higher Education, independent institutions of higher education, and private industry. The committee (1) designates its chairperson from among the members and (2) must meet at least quarterly and at other times the chairperson deems necessary.

The bill also makes technical and conforming changes.

EFFECTIVE DATE: July 1, 2024

BACKGROUND

CUTPA

By law, CUTPA prohibits businesses from engaging in unfair and deceptive acts or practices. It allows the DCP commissioner to issue regulations defining an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than $10,000, enter into consent agreements, ask the attorney general to seek injunctive relief, and accept voluntary statements of compliance. It also allows individuals to sue. Courts may issue restraining orders; award actual and punitive damages, costs, and reasonable attorney's fees; and impose civil penalties of up to $5,000 for willful violations and up to $25,000 for a restraining order violation.

Related Bills

sHB 5236, § 25, (File 103), favorably reported by the General Law Committee, among other things allows DCP to impose a civil penalty of up to $5,000 for CUTPA violations, after an administrative hearing.

HB 5421 (File 515), favorably reported by the Judiciary Committee, makes it a crime, under certain conditions, to intentionally disseminate a synthetic intimate image.

sHB 5450 (File 415), favorably reported by the Government Administration and Elections Committee, makes it a crime for a person to (1) distribute a communication with deceptive synthetic media or (2) enter into an agreement to distribute it.

sHB 5446 (File 372), favorably reported by the Energy and Technology Committee, requires the Office of Consumer Counsel to develop a plan for a Connecticut Internet for All program funded with revenue from the gross earnings tax on communications providers established under the bill.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 22 Nay 0 (03/12/2024)

Judiciary Committee

Joint Favorable
Yea 29 Nay 6 (04/22/2024)