

STATE OF NEW YORK

6953--B

2025-2026 Regular Sessions

IN SENATE

March 27, 2025

Introduced by Sens. GOUNARDES, BAILEY, BORRELLO, BRISPORT, FAHY, HARCHAM, HOYLMAN-SIGAL, JACKSON, KRUEGER, LIU, MAYER, PALUMBO, SALAZAR -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law, in relation to the training and use of artificial intelligence frontier models

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Short title. This act shall be known and may be cited as the "Responsible AI safety and education act" or "RAISE act".

§ 2. The general business law is amended by adding a new article 44-B to read as follows:

ARTICLE 44-B

RESPONSIBLE AI SAFETY AND EDUCATION (RAISE) ACT

Section 1420. Definitions.

1421. Transparency requirements regarding frontier model training and use.

1422. Violations.

1423. Duties and obligations.

1424. Scope.

1425. Severability.

§ 1420. Definitions. As used in this article, the following terms shall have the following meanings:

1. "Appropriate redactions" means redactions to a safety and security protocol that a developer may make when necessary to:

(a) protect public safety to the extent the developer can reasonably predict such risks;

(b) protect trade secrets;

EXPLANATION--Matter in italics (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD00047-15-5

1 (c) prevent the release of confidential information as required by
2 state or federal law;

3 (d) protect employee or customer privacy; or

4 (e) prevent the release of information otherwise controlled by state
5 or federal law.

6 2. "Artificial intelligence" means a machine-based system that can,
7 for a given set of human-defined objectives, make predictions, recommen-
8 dations, or decisions influencing real or virtual environments, and that
9 uses machine- and human-based inputs to perceive real and virtual envi-
10 ronments, abstract such perceptions into models through analysis in an
11 automated manner, and use model inference to formulate options for
12 information or action.

13 3. "Artificial intelligence model" means an information system or
14 component of an information system that implements artificial intelli-
15 gence technology and uses computational, statistical, or machine-learn-
16 ing techniques to produce outputs from a given set of inputs.

17 4. "Compute cost" means the cost incurred to pay for compute used in
18 the final training run of a model when calculated using the average
19 published market prices of cloud compute in the United States at the
20 start of training such model as reasonably assessed by the person doing
21 the training.

22 5. "Deploy" means to use a frontier model or to make a frontier model
23 foreseeably available to one or more third parties for use, modifica-
24 tion, copying, or a combination thereof with other software, except for
25 training or developing the frontier model, evaluating the frontier model
26 or other frontier models, or complying with federal or state laws.

27 6. "Frontier model" means either of the following:

28 (a) an artificial intelligence model trained using greater than 10²⁶
29 computational operations (e.g., integer or floating-point operations),
30 the compute cost of which exceeds one hundred million dollars; or

31 (b) an artificial intelligence model produced by applying knowledge
32 distillation to a frontier model as defined in paragraph (a) of this
33 subdivision, provided that the compute cost for such model produced by
34 applying knowledge distillation exceeds five million dollars.

35 7. "Critical harm" means the death or serious injury of one hundred or
36 more people or at least one billion dollars of damages to rights in
37 money or property caused or materially enabled by a large developer's
38 use, storage, or release of a frontier model, through either of the
39 following:

40 (a) The creation or use of a chemical, biological, radiological, or
41 nuclear weapon; or

42 (b) An artificial intelligence model engaging in conduct that does
43 both of the following:

44 (i) Acts with no meaningful human intervention; and

45 (ii) Would, if committed by a human, constitute a crime specified in
46 the penal law that requires intent, recklessness, or gross negligence,
47 or the solicitation or aiding and abetting of such a crime.

48 A harm inflicted by an intervening human actor shall not be deemed to
49 result from a developer's activities unless such activities were a
50 substantial factor in bringing about the harm, the intervening human
51 actor's conduct was reasonably foreseeable as a probable consequence of
52 the developer's activities, and could have been reasonably prevented or
53 mitigated through alternative design, or security measures, or safety
54 protocols.

55 8. "Knowledge distillation" means any supervised learning technique
56 that uses a larger artificial intelligence model or the output of a

1 larger artificial intelligence model to train a smaller artificial
2 intelligence model with similar or equivalent capabilities as the larger
3 artificial intelligence model.

4 9. "Large developer" means a person that has trained at least one
5 frontier model and has spent over one hundred million dollars in compute
6 costs in aggregate in training frontier models. Accredited colleges and
7 universities shall not be considered large developers under this article
8 to the extent that such colleges and universities are engaging in
9 academic research. If a person subsequently transfers full intellectual
10 property rights of the frontier model to another person (including the
11 right to resell the model) and retains none of those rights for them-
12 self, then the receiving person shall be considered the large developer
13 and shall be subject to the responsibilities and requirements of this
14 article after such transfer.

15 10. "Model weight" means a numerical parameter in an artificial intel-
16 ligence model that is adjusted through training and that helps determine
17 how inputs are transformed into outputs.

18 11. "Person" means an individual, proprietorship, firm, partnership,
19 joint venture, syndicate, business trust, company, corporation, limited
20 liability company, association, committee, or any other nongovernmental
21 organization or group of persons acting in concert.

22 12. "Safety and security protocol" means documented technical and
23 organizational protocols that:

24 (a) Describe reasonable protections and procedures that, if success-
25 fully implemented would appropriately reduce the risk of critical harm;

26 (b) Describe reasonable administrative, technical, and physical
27 cybersecurity protections for frontier models within the large develop-
28 er's control that, if successfully implemented, appropriately reduce the
29 risk of unauthorized access to, or misuse of, the frontier models lead-
30 ing to critical harm, including by sophisticated actors;

31 (c) Describe in detail the testing procedure to evaluate if the fron-
32 tier model poses an unreasonable risk of critical harm and whether the
33 frontier model could be misused, be modified, be executed with increased
34 computational resources, evade the control of its large developer or
35 user, be combined with other software or be used to create another fron-
36 tier model in a manner that would increase the risk of critical harm;

37 (d) Enable the large developer or third party to comply with the
38 requirements of this article; and

39 (e) Designate senior personnel to be responsible for ensuring compli-
40 ance.

41 13. "Safety incident" means a known incidence of critical harm or an
42 incident of the following kinds that occurs in such a way that it
43 provides demonstrable evidence of an increased risk of critical harm:

44 (a) A frontier model autonomously engaging in behavior other than at
45 the request of a user;

46 (b) Theft, misappropriation, malicious use, inadvertent release, unau-
47 thorized access, or escape of the model weights of a frontier model;

48 (c) The critical failure of any technical or administrative controls,
49 including controls limiting the ability to modify a frontier model; or

50 (d) Unauthorized use of a frontier model.

51 14. "Trade secret" means any form and type of financial, business,
52 scientific, technical, economic, or engineering information, including a
53 pattern, plan, compilation, program device, formula, design, prototype,
54 method, technique, process, procedure, program, or code, whether tangi-
55 ble or intangible, and whether or how stored, compiled, or memorialized

1 physically, electronically, graphically, photographically or in writing,
2 that:

3 (a) Derives independent economic value, actual or potential, from not
4 being generally known to, and not being readily ascertainable by proper
5 means by, other persons who can obtain economic value from its disclo-
6 sure or use; and

7 (b) Is the subject of efforts that are reasonable under the circum-
8 stances to maintain its secrecy.

9 § 1421. Transparency requirements regarding frontier model training
10 and use. 1. Before deploying a frontier model, the large developer of
11 such frontier model shall do all of the following:

12 (a) Implement a written safety and security protocol;

13 (b) Retain an unredacted copy of the safety and security protocol,
14 including records and dates of any updates or revisions. Such unredacted
15 copy of the safety and security protocol, including records and dates of
16 any updates or revisions, shall be retained for as long as a frontier
17 model is deployed plus five years;

18 (c) (i) Conspicuously publish a copy of the safety and security proto-
19 col with appropriate redactions and transmit a copy of such redacted
20 safety and security protocol to the attorney general and division of
21 homeland security and emergency services;

22 (ii) Grant the attorney general and division of homeland security and
23 emergency services or the attorney general access to the safety and
24 security protocol, with redactions only to the extent required by feder-
25 al law, upon request;

26 (d) Record, as and when reasonably possible, and retain for as long as
27 the frontier model is deployed plus five years information on the
28 specific tests and test results used in any assessment of the frontier
29 model required by this section or the developer's safety and security
30 protocol that provides sufficient detail for third parties to replicate
31 the testing procedure; and

32 (e) Implement appropriate safeguards to prevent unreasonable risk of
33 critical harm.

34 2. A large developer shall not deploy a frontier model if doing so
35 would create an unreasonable risk of critical harm.

36 3. A large developer shall conduct an annual review of any safety and
37 security protocol required by this section to account for any changes
38 to the capabilities of their frontier models and industry best practices
39 and, if necessary, make modifications to such safety and security proto-
40 col. If any material modifications are made, the large developer shall
41 publish the safety and security protocol in the same manner as required
42 pursuant to paragraph (c) of subdivision one of this section.

43 4. A large developer shall disclose each safety incident affecting the
44 frontier model to the attorney general and division of homeland security
45 and emergency services within seventy-two hours of the large developer
46 learning of the safety incident or within seventy-two hours of the large
47 developer learning facts sufficient to establish a reasonable belief
48 that a safety incident has occurred. Such disclosure shall include: (a)
49 the date of the safety incident; (b) the reasons the incident qualifies
50 as a safety incident as defined in subdivision thirteen of section four-
51 teen hundred twenty of this article; and (c) a short and plain statement
52 describing the safety incident.

53 5. A large developer shall not knowingly make false or materially
54 misleading statements or omissions in or regarding documents produced
55 pursuant to this section.

1 § 1422. Violations. 1. The attorney general may bring a civil action
2 for a violation of this article and to recover all of the following,
3 determined based on severity of the violation:

4 (a) For a violation of section fourteen hundred twenty-one of this
5 article, a civil penalty in an amount not exceeding ten million dollars
6 for a first violation and in an amount not exceeding thirty million
7 dollars for any subsequent violation.

8 (b) For a violation of section fourteen hundred twenty-one of this
9 article, injunctive or declaratory relief.

10 2. Nothing in this article shall be construed to establish a private
11 right of action associated with violations of this article.

12 3. Nothing in this subdivision shall be construed to prevent a large
13 developer from asserting that another person, entity, or factor may be
14 responsible for any alleged harm, injury, or damage resulting from a
15 critical harm or a violation of this article.

16 4. This section does not limit the application of other laws.

17 § 1423. Duties and obligations. The duties and obligations imposed by
18 this article are cumulative with any other duties or obligations imposed
19 under other law and shall not be construed to relieve any party from any
20 duties or obligations imposed under other law and do not limit any
21 rights or remedies under existing law.

22 § 1424. Scope. This article shall only apply to frontier models that
23 are developed, deployed, or operating in whole or in part in New York
24 state.

25 § 1425. Severability. If any clause, sentence, paragraph, subdivision,
26 section or part of this article shall be adjudged by any court of compe-
27 tent jurisdiction to be invalid, such judgment shall not affect, impair,
28 or invalidate the remainder thereof, but shall be confined in its opera-
29 tion to the clause, sentence, paragraph, subdivision, section, or part
30 thereof directly involved in the controversy in which such judgment
31 shall have been made.

32 § 3. This act shall take effect on the ninetieth day after it shall
33 have become a law.