

STATE OF NEW YORK

1962

2025-2026 Regular Sessions

IN SENATE

January 14, 2025

Introduced by Sen. GONZALEZ -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the general business law, in relation to preventing the use of artificial intelligence algorithms to discriminate against protected classes

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

1 Section 1. Short title. This act shall be known and may be cited as
2 the "New York artificial intelligence consumer protection act".

3 § 2. The general business law is amended by adding a new article 45-A
4 to read as follows:

ARTICLE 45-A

NEW YORK ARTIFICIAL INTELLIGENCE CONSUMER PROTECTION ACT

Section 1550. Definitions.

8 1551. Required documentation.

9 1552. Risk management.

10 1553. Technical documentation.

11 1554. Required disclosure.

12 1555. Preemption.

13 1556. Enforcement.

14 § 1550. Definitions. For the purposes of this article, the following
15 terms shall have the following meanings:

16 1. "Algorithmic discrimination":

17 (a) shall mean any condition in which the use of an artificial intel-
18 ligence decision system results in any unlawful differential treatment
19 or impact that disfavors any individual or group of individuals on the
20 basis of their actual or perceived age, color, disability, ethnicity,
21 genetic information, English language proficiency, national origin,
22 race, religion, reproductive health, sex, veteran status, or other clas-
23 sification protected pursuant to state or federal law; and

24 (b) shall not include:

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

LBD01361-01-5

1 (i) the offer, license, or use of a high-risk artificial intelligence
2 decision system by a developer or deployer for the sole purpose of:

3 (A) such developer's or deployer's self-testing to identify, mitigate,
4 or prevent discrimination or otherwise ensure compliance with state and
5 federal law; or

6 (B) expanding an applicant, customer, or participant pool to increase
7 diversity or redress historic discrimination; or

8 (ii) an act or omission by or on behalf of a private club or other
9 establishment not open to the general public, as set forth in title II
10 of the Civil Rights Act of 1964, 42 U.S.C. § 2000a(e), as amended.

11 2. "Artificial intelligence decision system" shall mean any computa-
12 tional process, derived from machine learning, statistical modeling,
13 data analytics, or artificial intelligence, that issues simplified
14 output, including any content, decision, prediction, or recommendation,
15 that is used to substantially assist or replace discretionary decision
16 making for making consequential decisions that impact consumers.

17 3. "Bias and governance audit" means an impartial evaluation by an
18 independent auditor, which shall include, at a minimum, the testing of
19 an artificial intelligence decision system to assess such system's
20 disparate impact on employees because of such employee's age, race,
21 creed, color, ethnicity, national origin, disability, citizenship or
22 immigration status, marital or familial status, military status, reli-
23 gion, or sex, including sexual orientation, gender identity, gender
24 expression, pregnancy, pregnancy outcomes, and reproductive healthcare
25 choices.

26 4. "Consequential decision" shall mean any decision that has a materi-
27 al legal or similarly significant effect on the provision or denial to
28 any consumer of, or the cost or terms of, any:

29 (a) education enrollment or education opportunity;

30 (b) employment or employment opportunity;

31 (c) financial or lending service;

32 (d) essential government service;

33 (e) health care service, as defined in section 42 U.S.C. § 324(d)(2),
34 as amended;

35 (f) housing or housing opportunity;

36 (g) insurance; or

37 (h) legal service.

38 5. "Consumer" shall mean any New York state resident.

39 6. "Deploy" shall mean to use a high-risk artificial intelligence
40 decision system.

41 7. "Deployer" shall mean any person doing business in this state that
42 deploys a high-risk artificial intelligence decision system.

43 8. "Developer" shall mean any person doing business in this state that
44 develops, or intentionally and substantially modifies, an artificial
45 intelligence decision system.

46 9. "General-purpose artificial intelligence model":

47 (a) shall mean any form of artificial intelligence decision system
48 that:

49 (i) displays significant generality;

50 (ii) is capable of competently performing a wide range of distinct
51 tasks; and

52 (iii) can be integrated into a variety of downstream applications or
53 systems; and

54 (b) shall not include any artificial intelligence model that is used
55 for development, prototyping, and research activities before such arti-
56 ficial intelligence model is released on the market.

1 10. "High-risk artificial intelligence decision system":

2 (a) shall mean any artificial intelligence decision system that, when
3 deployed, makes, or is a substantial factor in making, a consequential
4 decision; and

5 (b) shall not include:

6 (i) any artificial intelligence decision system that is intended to:

7 (A) perform any narrow procedural task; or

8 (B) detect decision-making patterns, or deviations from decision-mak-
9 ing patterns, unless such artificial intelligence decision system is
10 intended to replace or influence any assessment previously completed by
11 an individual without sufficient human review; or

12 (ii) unless the technology, when deployed, makes, or is a substantial
13 factor in making, a consequential decision:

14 (A) any anti-fraud technology that does not make use of facial recog-
15 niton technology;

16 (B) any artificial intelligence-enabled video game technology;

17 (C) any anti-malware, anti-virus, calculator, cybersecurity, database,
18 data storage, firewall, Internet domain registration, Internet-web-site
19 loading, networking, robocall-filtering, spam-filtering, spellchecking,
20 spreadsheet, web-caching, web-hosting, or similar technology;

21 (D) any technology that performs tasks exclusively related to an enti-
22 ty's internal management affairs, including, but not limited to, order-
23 ing office supplies or processing payments; or

24 (E) any technology that communicates with consumers in natural
25 language for the purpose of providing consumers with information, making
26 referrals or recommendations, and answering questions, and is subject to
27 an accepted use policy that prohibits generating content that is discrim-
28 inatory or harmful.

29 11. "Intentional and substantial modification":

30 (a) shall mean any deliberate change made to:

31 (i) an artificial intelligence decision system that results in any new
32 reasonably foreseeable risk of algorithmic discrimination; or

33 (ii) a general-purpose artificial intelligence model that:

34 (A) affects compliance of the general-purpose artificial intelligence
35 model;

36 (B) materially changes the purpose of the general-purpose artificial
37 intelligence model; or

38 (C) results in any new reasonably foreseeable risk of algorithmic
39 discrimination; and

40 (b) shall not include any change made to a high-risk artificial intel-
41 ligence decision system, or the performance of a high-risk artificial
42 intelligence decision system, if:

43 (i) the high-risk artificial intelligence decision system continues to
44 learn after such high-risk artificial intelligence decision system is:

45 (A) offered, sold, leased, licensed, given or otherwise made available
46 to a deployer; or

47 (B) deployed; and

48 (ii) such change:

49 (A) is made to such high-risk artificial intelligence decision system
50 as a result of any learning described in subparagraph (i) of this para-
51 graph;

52 (B) was predetermined by the deployer, or the third party contracted
53 by the deployer, when such deployer or third party completed the initial
54 impact assessment of such high-risk artificial intelligence decision
55 system pursuant to subdivision three of section one thousand five
56 hundred fifty-two of this article; and

1 (C) is included in the technical documentation for such high-risk
2 artificial intelligence decision system.

3 12. "Person" shall mean any individual, association, corporation,
4 limited liability company, partnership, trust or other legal entity
5 authorized to do business in this state.

6 13. "Red-teaming" shall mean an exercise that is conducted to identify
7 the potential adverse behaviors or outcomes of an artificial intelli-
8 gence decision system and how such behaviors or outcomes occur, and
9 stress test the safeguards against such adverse behaviors or outcomes.

10 14. "Substantial factor":

11 (a) shall mean a factor that:

12 (i) assists in making a consequential decision;

13 (ii) is capable of altering the outcome of a consequential decision;

14 and

15 (iii) is generated by an artificial intelligence decision system; and

16 (b) includes, but is not limited to, any use of an artificial intelli-
17 gence decision system to generate any content, decision, prediction, or
18 recommendation concerning a consumer that is used as a basis to make a
19 consequential decision concerning such consumer.

20 15. "Synthetic digital content" shall mean any digital content,
21 including, but not limited to, any audio, image, text, or video, that is
22 produced or manipulated by an artificial intelligence decision system,
23 including, but not limited to, a general-purpose artificial intelligence
24 model.

25 16. "Trade secret" shall mean any form and type of financial, busi-
26 ness, scientific, technical, economic, or engineering information,
27 including, but not limited to, a pattern, plan, compilation, program
28 device, formula, design, prototype, method, technique, process, proce-
29 dure, program, or code, whether tangible or intangible, and whether
30 stored, compiled, or memorialized physically, electronically, graph-
31 ically, photographically, or in writing, that:

32 (a) derives independent economic value, whether actual or potential,
33 from not being generally known to, or readily ascertainable by proper
34 means by, other persons who can obtain economic value from its disclo-
35 sure or use; and

36 (b) is the subject of efforts that are reasonable under the circum-
37 stances to maintain its secrecy.

38 § 1551. Required documentation. 1. (a) Beginning on January first, two
39 thousand twenty-seven, each developer of a high-risk artificial intelli-
40 gence decision system shall use reasonable care to protect consumers
41 from any known or reasonably foreseeable risks of algorithmic discrimi-
42 nation arising from the intended and contracted uses of a high-risk
43 artificial intelligence decision system. In any enforcement action
44 brought on or after such date by the attorney general pursuant to this
45 article, there shall be a rebuttable presumption that a developer used
46 reasonable care as required pursuant to this subdivision if:

47 (i) the developer complied with the provisions of this section; and

48 (ii) an independent third party identified by the attorney general
49 pursuant to paragraph (b) of this subdivision and retained by the devel-
50 oper completed bias and governance audits for the high-risk artificial
51 intelligence decision system.

52 (b) No later than January first, two thousand twenty-six, and at least
53 annually thereafter, the attorney general shall:

54 (i) identify independent third parties who, in the attorney general's
55 opinion, are qualified to complete bias and governance audits for the
56 purposes of subparagraph (ii) of paragraph (a) of this subdivision; and

1 (ii) publish a list of such independent third parties available on the
2 attorney general's website.

3 2. Beginning on January first, two thousand twenty-seven, and except
4 as provided in subdivision five of this section, a developer of a high-
5 risk artificial intelligence decision system shall make available to
6 each deployer or other developer the following information:

7 (a) A general statement describing the reasonably foreseeable uses,
8 and the known harmful or inappropriate uses, of such high-risk artifi-
9 cial intelligence decision system;

10 (b) Documentation disclosing:

11 (i) high-level summaries of the type of data used to train such high-
12 risk artificial intelligence decision system;

13 (ii) the known or reasonably foreseeable limitations of such high-risk
14 artificial intelligence decision system, including, but not limited to,
15 the known or reasonably foreseeable risks of algorithmic discrimination
16 arising from the intended uses of such high-risk artificial intelligence
17 decision system;

18 (iii) the purpose of such high-risk artificial intelligence decision
19 system;

20 (iv) the intended benefits and uses of such high-risk artificial
21 intelligence decision system; and

22 (v) any other information necessary to enable such deployer or other
23 developer to comply with the provisions of this article;

24 (c) Documentation describing:

25 (i) how such high-risk artificial intelligence decision system was
26 evaluated for performance, and mitigation of algorithmic discrimination,
27 before such high-risk artificial intelligence decision system was
28 offered, sold, leased, licensed, given, or otherwise made available to
29 such deployer or other developer;

30 (ii) the data governance measures used to cover the training datasets
31 and examine the suitability of data sources, possible biases, and appro-
32 priate mitigation;

33 (iii) the intended outputs of such high-risk artificial intelligence
34 decision system;

35 (iv) the measures such deployer or other developer has taken to miti-
36 gate any known or reasonably foreseeable risks of algorithmic discrimi-
37 nation that may arise from deployment of such high-risk artificial
38 intelligence decision system; and

39 (v) how such high-risk artificial intelligence decision system should
40 be used, not be used, and be monitored by an individual when such high-
41 risk artificial intelligence decision system is used to make, or as a
42 substantial factor in making, a consequential decision; and

43 (d) Any additional documentation that is reasonably necessary to
44 assist a deployer or other developer to:

45 (i) understand the outputs of such high-risk artificial intelligence
46 decision system; and

47 (ii) monitor the performance of such high-risk artificial intelligence
48 decision system for risks of algorithmic discrimination.

49 3. (a) Except as provided in subdivision five of this section, any
50 developer that, on or after January first, two thousand twenty-seven,
51 offers, sells, leases, licenses, gives, or otherwise makes available to
52 a deployer or other developer a high-risk artificial intelligence deci-
53 sion system shall, to the extent feasible, make available to such
54 deployers and other developers the documentation and information relat-
55 ing to such high-risk artificial intelligence decision system necessary
56 for a deployer, or the third party contracted by a deployer, to complete

1 an impact assessment pursuant to this article. The developer shall make
2 such documentation and information available through artifacts such as
3 model cards, dataset cards, or other impact assessments.

4 (b) A developer that also serves as a deployer for any high-risk arti-
5 ficial intelligence decision system shall not be required to generate
6 the documentation and information required pursuant to this section
7 unless such high-risk artificial intelligence decision system is
8 provided to an unaffiliated entity acting as a deployer.

9 4. (a) Beginning on January first, two thousand twenty-seven, each
10 developer shall publish, in a manner that is clear and readily avail-
11 able, on such developer's website, or a public use case inventory, a
12 statement summarizing:

13 (i) the types of high-risk artificial intelligence decision systems
14 that such developer:

15 (A) has developed or intentionally and substantially modified; and

16 (B) currently makes available to a deployer or other developer; and

17 (ii) how such developer manages any known or reasonably foreseeable
18 risks of algorithmic discrimination that may arise from the development
19 or intentional and substantial modification of the types of high-risk
20 artificial intelligence decision systems described in subparagraph (i)
21 of this subdivision.

22 (b) Each developer shall update the statement described in paragraph
23 (a) of this subdivision:

24 (i) as necessary to ensure that such statement remains accurate; and

25 (ii) no later than ninety days after the developer intentionally and
26 substantially modifies any high-risk artificial intelligence decision
27 system described in subparagraph (i) of paragraph (a) of this subdivi-
28 sion.

29 5. Nothing in subdivisions two or four of this section shall be
30 construed to require a developer to disclose any information:

31 (a) that is a trade secret or otherwise protected from disclosure
32 pursuant to state or federal law; or

33 (b) the disclosure of which would present a security risk to such
34 developer.

35 6. Beginning on January first, two thousand twenty-seven, the attorney
36 general may require that a developer disclose to the attorney general,
37 as part of an investigation conducted by the attorney general and in a
38 form and manner prescribed by the attorney general, the general state-
39 ment or documentation described in subdivision two of this section. The
40 attorney general may evaluate such general statement or documentation to
41 ensure compliance with the provisions of this section. In disclosing
42 such general statement or documentation to the attorney general pursuant
43 to this subdivision, the developer may designate such general statement
44 or documentation as including any information that is exempt from
45 disclosure pursuant to subdivision five of this section or article six
46 of the public officers law. To the extent such general statement or
47 documentation includes such information, such general statement or
48 documentation shall be exempt from disclosure. To the extent any infor-
49 mation contained in such general statement or documentation is subject
50 to the attorney-client privilege or work product protection, such
51 disclosure shall not constitute a waiver of such privilege or
52 protection.

53 § 1552. Risk management. 1. (a) Beginning on January first, two thou-
54 sand twenty-seven, each deployer of a high-risk artificial intelligence
55 decision system shall use reasonable care to protect consumers from any
56 known or reasonably foreseeable risks of algorithmic discrimination. In

1 any enforcement action brought on or after said date by the attorney
2 general pursuant to this article, there shall be a rebuttable presump-
3 tion that a deployer of a high-risk artificial intelligence decision
4 system used reasonable care as required pursuant to this subdivision if:

5 (i) the deployer complied with the provisions of this section; and

6 (ii) an independent third party identified by the attorney general
7 pursuant to paragraph (b) of this subdivision and retained by the
8 deployer completed bias and governance audits for the high-risk artifi-
9 cial intelligence decision system.

10 (b) No later than January first, two thousand twenty-seven, and at
11 least annually thereafter, the attorney general shall:

12 (i) identify the independent third parties who, in the attorney gener-
13 al's opinion, are qualified to complete bias and governance audits for
14 the purposes of subparagraph (ii) of paragraph (a) of this subdivision;
15 and

16 (ii) make a list of such independent third parties available on the
17 attorney general's web site.

18 2. (a) Beginning on January first, two thousand twenty-seven, and
19 except as provided in subdivision seven of this section, each deployer
20 of a high-risk artificial intelligence decision system shall implement
21 and maintain a risk management policy and program to govern such
22 deployer's deployment of the high-risk artificial intelligence decision
23 system. The risk management policy and program shall specify and incor-
24 porate the principles, processes, and personnel that the deployer shall
25 use to identify, document, and mitigate any known or reasonably foresee-
26 able risks of algorithmic discrimination. The risk management policy
27 shall be the product of an iterative process, the risk management
28 program shall be an iterative process and both the risk management poli-
29 cy and program shall be planned, implemented, and regularly and system-
30 atically reviewed and updated over the lifecycle of the high-risk arti-
31 ficial intelligence decision system. Each risk management policy and
32 program implemented and maintained pursuant to this subdivision shall be
33 reasonable, considering:

34 (i) the guidance and standards set forth in the latest version of:

35 (A) the "Artificial Intelligence Risk Management Framework" published
36 by the national institute of standards and technology;

37 (B) ISO or IEC 42001 of the international organization for standardi-
38 zation; or

39 (C) a nationally or internationally recognized risk management frame-
40 work for artificial intelligence decision systems, other than the guid-
41 ance and standards specified in clauses (A) and (B) of this subpara-
42 graph, that imposes requirements that are substantially equivalent to,
43 and at least as stringent as, the requirements established pursuant to
44 this section for risk management policies and programs;

45 (ii) the size and complexity of the deployer;

46 (iii) the nature and scope of the high-risk artificial intelligence
47 decision systems deployed by the deployer, including, but not limited
48 to, the intended uses of such high-risk artificial intelligence decision
49 systems; and

50 (iv) the sensitivity and volume of data processed in connection with
51 the high-risk artificial intelligence decision systems deployed by the
52 deployer.

53 (b) A risk management policy and program implemented and maintained
54 pursuant to paragraph (a) of this subdivision may cover multiple high-
55 risk artificial intelligence decision systems deployed by the deployer.

1 3. (a) Except as provided in paragraphs (c) and (d) of this subdivi-
2 vision and subdivision seven of this section:

3 (i) a deployer that deploys a high-risk artificial intelligence deci-
4 sion system on or after January first, two thousand twenty-seven, or a
5 third party contracted by the deployer, shall complete an impact assess-
6 ment of the high-risk artificial intelligence decision system; and

7 (ii) beginning on January first, two thousand twenty-seven, a deploy-
8 er, or a third party contracted by the deployer, shall complete an
9 impact assessment of a deployed high-risk artificial intelligence deci-
10 sion system:

11 (A) at least annually; and

12 (B) no later than ninety days after an intentional and substantial
13 modification to such high-risk artificial intelligence decision system
14 is made available.

15 (b) (i) Each impact assessment completed pursuant to this subdivision
16 shall include, at a minimum and to the extent reasonably known by, or
17 available to, the deployer:

18 (A) a statement by the deployer disclosing the purpose, intended use
19 cases and deployment context of, and benefits afforded by, the high-risk
20 artificial intelligence decision system;

21 (B) an analysis of whether the deployment of the high-risk artificial
22 intelligence decision system poses any known or reasonably foreseeable
23 risks of algorithmic discrimination and, if so, the nature of such algo-
24 rithmic discrimination and the steps that have been taken to mitigate
25 such risks;

26 (C) A description of:

27 (I) the categories of data the high-risk artificial intelligence deci-
28 sion system processes as inputs; and

29 (II) the outputs such high-risk artificial intelligence decision
30 system produces;

31 (D) if the deployer used data to customize the high-risk artificial
32 intelligence decision system, an overview of the categories of data the
33 deployer used to customize such high-risk artificial intelligence deci-
34 sion system;

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

37 (F) a description of any transparency measures taken concerning the
38 high-risk artificial intelligence decision system, including, but not
39 limited to, any measures taken to disclose to a consumer that such high-
40 risk artificial intelligence decision system is in use when such high-
41 risk artificial intelligence decision system is in use; and

42 (G) a description of the post-deployment monitoring and user safe-
43 guards provided concerning such high-risk artificial intelligence deci-
44 sion system, including, but not limited to, the oversight, use, and
45 learning process established by the deployer to address issues arising
46 from deployment of such high-risk artificial intelligence decision
47 system.

48 (ii) In addition to the statement, analysis, descriptions, overview,
49 and metrics required pursuant to subparagraph (i) of this paragraph, an
50 impact assessment completed pursuant to this subdivision following an
51 intentional and substantial modification made to a high-risk artificial
52 intelligence decision system on or after January first, two thousand
53 twenty-seven, shall include a statement disclosing the extent to which
54 the high-risk artificial intelligence decision system was used in a
55 manner that was consistent with, or varied from, the developer's
56 intended uses of such high-risk artificial intelligence decision system.

1 (c) A single impact assessment may address a comparable set of high-
2 risk artificial intelligence decision systems deployed by a deployer.

3 (d) If a deployer, or a third party contracted by the deployer,
4 completes an impact assessment for the purpose of complying with another
5 applicable law or regulation, such impact assessment shall be deemed to
6 satisfy the requirements established in this subdivision if such impact
7 assessment is reasonably similar in scope and effect to the impact
8 assessment that would otherwise be completed pursuant to this subdivi-
9 sion.

10 (e) A deployer shall maintain the most recently completed impact
11 assessment of a high-risk artificial intelligence decision system as
12 required pursuant to this subdivision, all records concerning each such
13 impact assessment and all prior impact assessments, if any, for a period
14 of at least three years following the final deployment of the high-risk
15 artificial intelligence decision system.

16 4. Except as provided in subdivision seven of this section, a deploy-
17 er, or a third party contracted by the deployer, shall review, no later
18 than January first, two thousand twenty-seven, and at least annually
19 thereafter, the deployment of each high-risk artificial intelligence
20 decision system deployed by the deployer to ensure that such high-risk
21 artificial intelligence decision system is not causing algorithmic
22 discrimination.

23 5. (a) Beginning on January first, two thousand twenty-seven, and
24 before a deployer deploys a high-risk artificial intelligence decision
25 system to make, or be a substantial factor in making, a consequential
26 decision concerning a consumer, the deployer shall:

27 (i) notify the consumer that the deployer has deployed a high-risk
28 artificial intelligence decision system to make, or be a substantial
29 factor in making, such consequential decision; and

30 (ii) provide to the consumer:

31 (A) a statement disclosing:

32 (I) the purpose of such high-risk artificial intelligence decision
33 system; and

34 (II) the nature of such consequential decision;

35 (B) contact information for such deployer;

36 (C) a description, in plain language, of such high-risk artificial
37 intelligence decision system; and

38 (D) instructions on how to access the statement made available pursu-
39 ant to paragraph (a) of subdivision six of this section.

40 (b) Beginning on January first, two thousand twenty-seven, a deployer
41 that has deployed a high-risk artificial intelligence decision system to
42 make, or as a substantial factor in making, a consequential decision
43 concerning a consumer shall, if such consequential decision is adverse
44 to the consumer, provide to such consumer:

45 (i) a statement disclosing the principal reason or reasons for such
46 adverse consequential decision, including, but not limited to:

47 (A) the degree to which, and manner in which, the high-risk artificial
48 intelligence decision system contributed to such adverse consequential
49 decision;

50 (B) the type of data that was processed by such high-risk artificial
51 intelligence decision system in making such adverse consequential deci-
52 sion; and

53 (C) the source of such data; and

54 (ii) an opportunity to:

1 (A) correct any incorrect personal data that the high-risk artificial
2 intelligence decision system processed in making, or as a substantial
3 factor in making, such adverse consequential decision; and

4 (B) appeal such adverse consequential decision, which shall, if tech-
5 nically feasible, allow for human review unless providing such opportu-
6 nity is not in the best interest of such consumer, including, but not
7 limited to, in instances in which any delay might pose a risk to the
8 life or safety of such consumer.

9 (c) The deployer shall provide the notice, statements, information,
10 description, and instructions required pursuant to paragraphs (a) and
11 (b) of this subdivision:

12 (i) directly to the consumer;

13 (ii) in plain language;

14 (iii) in all languages in which such deployer, in the ordinary course
15 of such deployer's business, provides contracts, disclaimers, sale
16 announcements, and other information to consumers; and

17 (iv) in a format that is accessible to consumers with disabilities.

18 6. (a) Beginning on January first, two thousand twenty-seven, and
19 except as provided in subdivision seven of this section, each deployer
20 shall make available, in a manner that is clear and readily available on
21 such deployer's website, a statement summarizing:

22 (i) the types of high-risk artificial intelligence decision systems
23 that are currently deployed by such deployer;

24 (ii) how such deployer manages any known or reasonably foreseeable
25 risks of algorithmic discrimination that may arise from deployment of
26 each high-risk artificial intelligence decision system described in
27 subparagraph (i) of this paragraph; and

28 (iii) in detail, the nature, source and extent of the information
29 collected and used by such deployer.

30 (b) Each deployer shall periodically update the statement required
31 pursuant to paragraph (a) of this subdivision.

32 7. The provisions of subdivisions two, three, four, and six of this
33 section shall not apply to a deployer if, at the time the deployer
34 deploys a high-risk artificial intelligence decision system, and at all
35 times while the high-risk artificial intelligence decision system is
36 deployed:

37 (a) the deployer:

38 (i) has entered into a contract with the developer in which the devel-
39 oper has agreed to assume the deployer's duties pursuant to subdivisions
40 two, three, four, or six of this section; and

41 (ii) does not exclusively use such deployer's own data to train such
42 high-risk artificial intelligence decision system;

43 (b) such high-risk artificial intelligence decision system:

44 (i) is used for the intended uses that are disclosed to such deployer
45 pursuant to subparagraph (iv) of paragraph (b) of subdivision two of
46 section one thousand five hundred fifty-one of this article; and

47 (ii) continues learning based on a broad range of data sources and not
48 solely based on the deployer's own data; and

49 (c) such deployer makes available to consumers any impact assessment
50 that:

51 (i) the developer of such high-risk artificial intelligence decision
52 system has completed and provided to such deployer; and

53 (ii) includes information that is substantially similar to the infor-
54 mation included in the statement, analysis, descriptions, overview, and
55 metrics required pursuant to subparagraph (i) of paragraph (b) of subdi-
56 vision three of this section.

1 8. Nothing in this subdivision or subdivisions two, three, four, five,
2 or six of this section shall be construed to require a deployer to
3 disclose any information that is a trade secret or otherwise protected
4 from disclosure pursuant to state or federal law. If a deployer with-
5 holds any information from a consumer pursuant this subdivision, the
6 deployer shall send notice to such consumer disclosing:

7 (a) that the deployer is withholding such information from such
8 consumer; and

9 (b) the basis for the deployer's decision to withhold such information
10 from such consumer.

11 9. Beginning on January first, two thousand twenty-seven, the attorney
12 general may require that a deployer, or a third party contracted by the
13 deployer pursuant to subdivision three of this section, as applicable,
14 disclose to the attorney general, as part of an investigation conducted
15 by the attorney general, no later than ninety days after a request by
16 the attorney general, and in a form and manner prescribed by the attor-
17 ney general, the risk management policy implemented pursuant to subdivi-
18 sion two of this section, the impact assessment completed pursuant to
19 subdivision three of this section; or records maintained pursuant to
20 paragraph (e) of subdivision three of this section. The attorney general
21 may evaluate such risk management policy, impact assessment or records
22 to ensure compliance with the provisions of this section. In disclosing
23 such risk management policy, impact assessment or records to the attor-
24 ney general pursuant to this subdivision, the deployer or third-party
25 contractor, as applicable, may designate such risk management policy,
26 impact assessment or records as including any information that is exempt
27 from disclosure pursuant to subdivision eight of this section or article
28 six of the public officers law. To the extent such risk management poli-
29 cy, impact assessment, or records include such information, such risk
30 management policy, impact assessment, or records shall be exempt from
31 disclosure. To the extent any information contained in such risk manage-
32 ment policy, impact assessment, or record is subject to the attorney-
33 client privilege or work product protection, such disclosure shall not
34 constitute a waiver of such privilege or protection.

35 § 1553. Technical documentation. 1. Beginning on January first, two
36 thousand twenty-seven, each developer of a general-purpose artificial
37 intelligence model shall, except as provided in subdivision two of this
38 section:

39 (a) create and maintain technical documentation for the general-pur-
40 pose artificial intelligence model, which shall:

41 (i) include:

42 (A) the training and testing processes for such general-purpose arti-
43 ficial intelligence model; and

44 (B) the results of an evaluation of such general-purpose artificial
45 intelligence model performed to determine whether such general-purpose
46 artificial intelligence model is in compliance with the provisions of
47 this article;

48 (ii) include, as appropriate, considering the size and risk profile of
49 such general-purpose artificial intelligence model, at least:

50 (A) the tasks such general-purpose artificial intelligence model is
51 intended to perform;

52 (B) the type and nature of artificial intelligence decision systems in
53 which such general-purpose artificial intelligence model is intended to
54 be integrated;

55 (C) acceptable use policies for such general-purpose artificial intel-
56 ligence model;

1 (D) the date such general-purpose artificial intelligence model is
2 released;

3 (E) the methods by which such general-purpose artificial intelligence
4 model is distributed; and

5 (F) the modality and format of inputs and outputs for such general-
6 purpose artificial intelligence model; and

7 (iii) be reviewed and revised at least annually, or more frequently,
8 as necessary to maintain the accuracy of such technical documentation;
9 and

10 (b) create, implement, maintain and make available to persons that
11 intend to integrate such general-purpose artificial intelligence model
12 into such persons' artificial intelligence decision systems documenta-
13 tion and information that:

14 (i) enables such persons to:

15 (A) understand the capabilities and limitations of such general-pur-
16 pose artificial intelligence model; and

17 (B) comply with such persons' obligations pursuant to this article;

18 (ii) discloses, at a minimum:

19 (A) the technical means required for such general-purpose artificial
20 intelligence model to be integrated into such persons' artificial intel-
21 ligence decision systems;

22 (B) the information listed in subparagraph (ii) of paragraph (a) of
23 this subdivision; and

24 (iii) except as provided in subdivision two of this section, is
25 reviewed and revised at least annually, or more frequently, as necessary
26 to maintain the accuracy of such documentation and information.

27 2. (a) The provisions of paragraph (a) and subparagraph (iii) of para-
28 graph (b) of subdivision one of this section shall not apply to a devel-
29 oper that develops, or intentionally and substantially modifies, a
30 general-purpose artificial intelligence model on or after January first,
31 two thousand twenty-seven, if:

32 (i) (A) the developer releases such general-purpose artificial intel-
33 ligence model under a free and open-source license that allows for:

34 (I) access to, and modification, distribution, and usage of, such
35 general-purpose artificial intelligence model; and

36 (II) the parameters of such general-purpose artificial intelligence
37 model to be made publicly available pursuant to clause (B) of this
38 subparagraph; and

39 (B) unless such general-purpose artificial intelligence model is
40 deployed as a high-risk artificial intelligence decision system, the
41 parameters of such general-purpose artificial intelligence model,
42 including, but not limited to, the weights and information concerning
43 the model architecture and model usage for such general-purpose artifi-
44 cial intelligence model, are made publicly available; or

45 (ii) the general-purpose artificial intelligence model is:

46 (A) not offered for sale in the market;

47 (B) not intended to interact with consumers; and

48 (C) solely utilized:

49 (I) for an entity's internal purposes; or

50 (II) pursuant to an agreement between multiple entities for such enti-
51 ties' internal purposes.

52 (b) The provisions of this section shall not apply to a developer that
53 develops, or intentionally and substantially modifies, a general-purpose
54 artificial intelligence model on or after January first, two thousand
55 twenty-seven, if such general purpose artificial intelligence model
56 performs tasks exclusively related to an entity's internal management

1 affairs, including, but not limited to, ordering office supplies or
2 processing payments.

3 (c) A developer that takes any action under an exemption pursuant to
4 paragraph (a) or (b) of this subdivision shall bear the burden of demon-
5 strating that such action qualifies for such exemption.

6 (d) A developer that is exempt pursuant to subparagraph (ii) of para-
7 graph (a) of this subdivision shall establish and maintain an artificial
8 intelligence risk management framework, which shall:

9 (i) be the product of an iterative process and ongoing efforts; and

10 (ii) include, at a minimum:

11 (A) an internal governance function;

12 (B) a map function that shall establish the context to frame risks;

13 (C) a risk management function; and

14 (D) a function to measure identified risks by assessing, analyzing and
15 tracking such risks.

16 3. Nothing in subdivision one of this section shall be construed to
17 require a developer to disclose any information that is a trade secret
18 or otherwise protected from disclosure pursuant to state or federal law.

19 4. Beginning on January first, two thousand twenty-seven, the attorney
20 general may require that a developer disclose to the attorney general,
21 as part of an investigation conducted by the attorney general, no later
22 than ninety days after a request by the attorney general and in a form
23 and manner prescribed by the attorney general, any documentation main-
24 tained pursuant to this section. The attorney general may evaluate such
25 documentation to ensure compliance with the provisions of this section.
26 In disclosing any documentation to the attorney general pursuant to this
27 subdivision, the developer may designate such documentation as including
28 any information that is exempt from disclosure pursuant to subdivision
29 three of this section or article six of the public officers law. To the
30 extent such documentation includes such information, such documentation
31 shall be exempt from disclosure. To the extent any information contained
32 in such documentation is subject to the attorney-client privilege or
33 work product protection, such disclosure shall not constitute a waiver
34 of such privilege or protection.

35 § 1554. Required disclosure. 1. Beginning on January first, two thou-
36 sand twenty-seven, and except as provided in subdivision two of this
37 section, each person doing business in this state, including, but not
38 limited to, each deployer that deploys, offers, sells, leases, licenses,
39 gives, or otherwise makes available, as applicable, any artificial
40 intelligence decision system that is intended to interact with consumers
41 shall ensure that it is disclosed to each consumer who interacts with
42 such artificial intelligence decision system that such consumer is
43 interacting with an artificial intelligence decision system.

44 2. No disclosure shall be required pursuant to subdivision one of this
45 section under circumstances in which a reasonable person would deem it
46 obvious that such person is interacting with an artificial intelligence
47 decision system.

48 § 1555. Preemption. 1. Nothing in this article shall be construed to
49 restrict a developer's, deployer's, or other person's ability to:

50 (a) comply with federal, state or municipal law;

51 (b) comply with a civil, criminal or regulatory inquiry, investi-
52 gation, subpoena, or summons by a federal, state, municipal, or other
53 governmental authority;

54 (c) cooperate with a law enforcement agency concerning conduct or
55 activity that the developer, deployer, or other person reasonably and in
56 good faith believes may violate federal, state, or municipal law;

1 (d) investigate, establish, exercise, prepare for, or defend a legal
2 claim;

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

5 (f) (i) by any means other than facial recognition technology,
6 prevent, detect, protect against, or respond to:

7 (A) a security incident;

8 (B) a malicious or deceptive activity; or

9 (C) identity theft, fraud, harassment or any other illegal activity;

10 (ii) investigate, report, or prosecute the persons responsible for any
11 action described in subparagraph (i) of this paragraph; or

12 (iii) preserve the integrity or security of systems;

13 (g) engage in public or peer-reviewed scientific or statistical
14 research in the public interest that:

15 (i) adheres to all other applicable ethics and privacy laws; and

16 (ii) is conducted in accordance with:

17 (A) part forty-six of title forty-five of the code of federal regu-
18 lations, as amended; or

19 (B) relevant requirements established by the federal food and drug
20 administration;

21 (h) conduct research, testing, and development activities regarding an
22 artificial intelligence decision system or model, other than testing
23 conducted pursuant to real world conditions, before such artificial
24 intelligence decision system or model is placed on the market, deployed,
25 or put into service, as applicable;

26 (i) effectuate a product recall;

27 (j) identify and repair technical errors that impair existing or
28 intended functionality; or

29 (k) assist another developer, deployer, or person with any of the
30 obligations imposed pursuant to this article.

31 2. The obligations imposed on developers, deployers, or other persons
32 pursuant to this article shall not apply where compliance by the devel-
33 oper, deployer, or other person with the provisions of this article
34 would violate an evidentiary privilege pursuant to state law.

35 3. Nothing in this article shall be construed to impose any obligation
36 on a developer, deployer, or other person that adversely affects the
37 rights or freedoms of any person, including, but not limited to, the
38 rights of any person:

39 (a) to freedom of speech or freedom of the press guaranteed in:

40 (i) the first amendment to the United States constitution; and

41 (ii) section eight of the New York state constitution; or

42 (b) pursuant to section seventy-nine-h of the civil rights law.

43 4. Nothing in this article shall be construed to apply to any develop-
44 er, deployer, or other person:

45 (a) insofar as such developer, deployer or other person develops,
46 deploys, puts into service, or intentionally and substantially modifies,
47 as applicable, a high-risk artificial intelligence decision system:

48 (i) that has been approved, authorized, certified, cleared, developed,
49 or granted by:

50 (A) a federal agency, including, but not limited to, the federal food
51 and drug administration or the federal aviation administration, acting
52 within the scope of such federal agency's authority; or

53 (B) a regulated entity subject to supervision and regulation by the
54 federal housing finance agency; or

55 (ii) in compliance with standards that are:

56 (A) established by:

1 (I) any federal agency, including, but not limited to, the federal
2 office of the national coordinator for health information technology; or
3 (II) a regulated entity subject to supervision and regulation by the
4 federal housing finance agency; and

5 (B) substantially equivalent to, and at least as stringent as, the
6 standards established pursuant to this article;

7 (b) conducting research to support an application:

8 (i) for approval or certification from any federal agency, including,
9 but not limited to, the federal food and drug administration, the feder-
10 al aviation administration, or the federal communications commission; or

11 (ii) that is otherwise subject to review by any federal agency;

12 (c) performing work pursuant to, or in connection with, a contract
13 with the federal department of commerce, the federal department of
14 defense, or the national aeronautics and space administration, unless
15 such developer, deployer, or other person is performing such work on a
16 high-risk artificial intelligence decision system that is used to make,
17 or as a substantial factor in making, a decision concerning employment
18 or housing; or

19 (d) that is a covered entity, as defined by the health insurance
20 portability and accountability act of 1996 and the regulations promul-
21 gated thereunder, as amended, and providing health care recommendations
22 that:

23 (i) are generated by an artificial intelligence decision system;

24 (ii) require a health care provider to take action to implement such
25 recommendations; and

26 (iii) are not considered to be high risk.

27 5. Nothing in this article shall be construed to apply to any artifi-
28 cial intelligence decision system that is acquired by or for the federal
29 government or any federal agency or department, including, but not
30 limited to, the federal department of commerce, the federal department
31 of defense, or the national aeronautics and space administration, unless
32 such artificial intelligence decision system is a high-risk artificial
33 intelligence decision system that is used to make, or as a substantial
34 factor in making, a decision concerning employment or housing.

35 6. Any insurer, as defined by section five hundred one of the insur-
36 ance law, or fraternal benefit society, as defined by section four thou-
37 sand five hundred one of the insurance law, shall be deemed to be in
38 full compliance with the provisions of this article if such insurer or
39 fraternal benefit society has implemented and maintains a written arti-
40 ficial intelligence decision systems program in accordance with all
41 requirements established by the superintendent of financial services.

42 7. (a) Any bank, out-of-state bank, New York credit union, federal
43 credit union, or out-of-state credit union, or any affiliate or subsid-
44 iary thereof, shall be deemed to be in full compliance with the
45 provisions of this article if such bank, out-of-state bank, New York
46 credit union, federal credit union, out-of-state credit union, affil-
47 iate, or subsidiary is subject to examination by any state or federal
48 prudential regulator pursuant to any published guidance or regulations
49 that apply to the use of high-risk artificial intelligence decision
50 systems, and such guidance or regulations:

51 (i) impose requirements that are substantially equivalent to, and at
52 least as stringent as, the requirements of this article; and

53 (ii) at a minimum, require such bank, out-of-state bank, New York
54 credit union, federal credit union, out-of-state credit union, affil-
55 iate, or subsidiary to:

1 (A) regularly audit such bank's, out-of-state bank's, New York credit
2 union's, federal credit union's, out-of-state credit union's, affil-
3 iate's, or subsidiary's use of high-risk artificial intelligence deci-
4 sion systems for compliance with state and federal anti-discrimination
5 laws and regulations applicable to such bank, out-of-state bank, New
6 York credit union, federal credit union, out-of-state credit union,
7 affiliate, or subsidiary; and

8 (B) mitigate any algorithmic discrimination caused by the use of a
9 high-risk artificial intelligence decision system, or any risk of algo-
10 rithmic discrimination that is reasonably foreseeable as a result of the
11 use of a high-risk artificial intelligence decision system.

12 (b) For the purposes of this subdivision, the following terms shall
13 have the following meanings:

14 (i) "Affiliate" shall have the same meaning as set forth in section
15 nine hundred twelve of the business corporation law.

16 (ii) "Bank" shall have the same meaning as set forth in section two of
17 the banking law.

18 (iii) "Credit union" shall have the same meaning as set forth in
19 section two of the banking law.

20 (iv) "Out-of-state bank" shall have the same meaning as set forth in
21 section two hundred twenty-two of the banking law.

22 (v) "Subsidiary" shall have the same meaning as set forth in section
23 one hundred forty-one of the banking law.

24 8. If a developer, deployer, or other person engages in any action
25 under an exemption pursuant to subdivisions one, two, three, four, five,
26 six, or seven of this section, the developer, deployer, or other person
27 bears the burden of demonstrating that such action qualifies for such
28 exemption.

29 § 1556. Enforcement. 1. The attorney general shall have exclusive
30 authority to enforce the provisions of this article.

31 2. Except as provided in subdivision six of this section, during the
32 period beginning on January first, two thousand twenty-seven, and ending
33 on January first, two thousand twenty-eight, the attorney general shall,
34 prior to initiating any action for a violation of this section, issue a
35 notice of violation to the developer, deployer, or other person if the
36 attorney general determines that it is possible to cure such violation.
37 If the developer, deployer, or other person fails to cure such violation
38 within sixty days after receipt of such notice of violation, the attor-
39 ney general may bring an action pursuant to this section.

40 3. Except as provided in subdivision six of this section, beginning on
41 January first, two thousand twenty-eight, the attorney general may, in
42 determining whether to grant a developer, deployer, or other person the
43 opportunity to cure a violation described in subdivision two of this
44 section, consider:

45 (a) the number of violations;

46 (b) the size and complexity of the developer, deployer, or other
47 person;

48 (c) the nature and extent of the developer's, deployer's, or other
49 person's business;

50 (d) the substantial likelihood of injury to the public;

51 (e) the safety of persons or property; and

52 (f) whether such violation was likely caused by human or technical
53 error.

54 4. Nothing in this article shall be construed as providing the basis
55 for a private right of action for violations of the provisions of this
56 article.

1 5. Except as provided in subdivisions one, two, three, four, and six
2 of this section, a violation of the requirements established in this
3 article shall constitute an unfair trade practice for purposes of
4 section three hundred forty-nine of this chapter and shall be enforced
5 solely by the attorney general; provided, however, that subdivision (h)
6 of section three hundred forty-nine of this chapter shall not apply to
7 any such violation.

8 6. (a) In any action commenced by the attorney general for any
9 violation of this article, it shall be an affirmative defense that the
10 developer, deployer, or other person:

11 (i) discovers a violation of any provision of this article through
12 red-teaming;

13 (ii) no later than sixty days after discovering such violation through
14 red-teaming:

15 (A) cures such violation; and

16 (B) provides to the attorney general, in a form and manner prescribed
17 by the attorney general, notice that such violation has been cured and
18 evidence that any harm caused by such violation has been mitigated; and

19 (iii) is otherwise in compliance with the latest version of:

20 (A) the Artificial Intelligence Risk Management Framework published by
21 the national institute of standards and technology;

22 (B) ISO/IEC 42001 of the international organization for standardi-
23 zation and the international electrotechnical commission;

24 (C) a nationally or internationally recognized risk management frame-
25 work for artificial intelligence decision systems, other than the risk
26 management frameworks described in clauses (A) and (B) of this subpara-
27 graph, that imposes requirements that are substantially equivalent to,
28 and at least as stringent as, the requirements established pursuant to
29 this article; or

30 (D) any risk management framework for artificial intelligence decision
31 systems that is substantially equivalent to, and at least as stringent
32 as, the risk management frameworks described in clauses (A), (B), and
33 (C) of this subparagraph.

34 (b) The developer, deployer, or other person bears the burden of
35 demonstrating to the attorney general that the requirements established
36 pursuant to paragraph (a) of this subdivision have been satisfied.

37 (c) Nothing in this article, including, but not limited to, the
38 enforcement authority granted to the attorney general pursuant to this
39 section, shall be construed to preempt or otherwise affect any right,
40 claim, remedy, presumption, or defense available at law or in equity.
41 Any rebuttable presumption or affirmative defense established pursuant
42 to this article shall apply only to an enforcement action brought by the
43 attorney general pursuant to this section and shall not apply to any
44 right, claim, remedy, presumption, or defense available at law or in
45 equity.

46 § 3. This act shall take effect on the two hundred seventieth day
47 after it shall have become a law.