

ASSEMBLY, No. 5430

STATE OF NEW JERSEY 218th LEGISLATURE

INTRODUCED MAY 20, 2019

Sponsored by:

Assemblyman ANDREW ZWICKER

District 16 (Hunterdon, Mercer, Middlesex and Somerset)

Assemblyman HERB CONAWAY, JR.

District 7 (Burlington)

SYNOPSIS

“New Jersey Algorithmic Accountability Act”; requires certain businesses to conduct automated decision and data protection impact assessments.

CURRENT VERSION OF TEXT

As introduced.



1 AN ACT requiring certain businesses to conduct automated decision
2 and data protection impact assessments and supplementing Title
3 56 of the Revised Statutes.

4

5 **BE IT ENACTED** *by the Senate and General Assembly of the State*
6 *of New Jersey:*

7

8 1. This act shall be known and may be cited as the “New Jersey
9 Algorithmic Accountability Act.”

10

11 2. As used in P.L. , c. (C.) (pending before the
12 Legislature as this bill):

13 “Automated decision system” means a computational process,
14 including one derived from machine learning, statistics, or other
15 data processing or artificial intelligence techniques, that makes a
16 decision or facilitates human decision making and that impacts
17 consumers.

18 “Automated decision system impact assessment” means a study
19 evaluating an automated decision system and the automated
20 decision system’s development process, including the design and
21 training data of the automated decision system, for impacts on
22 accuracy, fairness, bias, discrimination, privacy, and security that
23 shall include, but not be limited to:

24 a detailed description of the automated decision system, its
25 design, decision training, data collection, and purpose;

26 a cost-benefit analysis of the automated decision system in light
27 of its purpose, taking into account relevant factors, including:

28 data minimization practices;

29 the duration for which personally identifiable information and
30 the results of the automated decision system are stored;

31 what information about the automated decision system is
32 available to consumers;

33 the extent to which consumers have access to the results of the
34 automated decision system and may correct or object to its results;
35 and

36 the recipients of the results of the decisions of the automated
37 decision system;

38 an assessment of the risks posed by the automated decision
39 system to the privacy or security of personally identifiable
40 information of consumers and the risks that the automated decision
41 system may result in or contribute to inaccurate, unfair, biased, or
42 discriminatory decisions impacting consumers; and

43 the measures the covered entity will employ to minimize the
44 risks posed, including technological and physical safeguards.

45 “Consumer” means an individual within this State who provides,
46 either knowingly or unknowingly, personally identifiable
47 information to a covered entity.

1 “Covered entity” means a corporation, partnership, firm,
2 enterprise, franchise, association, trust, sole proprietorship, union,
3 political organization, or other legal entity other than a State agency
4 or any political subdivision thereof, federal agency, or any
5 contractor or subcontractor employed by a State agency, political
6 subdivision thereof, or federal agency, that does business in this
7 State and that:

8 had greater than \$50,000,000 in average annual gross receipts for
9 the three taxable-year period preceding the most recent fiscal year,
10 as determined in accordance with paragraphs (2) and (3) of section
11 448(c) of the Internal Revenue Code, 26 U.S.C. s.448;

12 possesses or controls personally identifiable information on more
13 than:

14 1,000,000 consumers; or

15 1,000,000 consumer computers or mobile telecommunications
16 service devices;

17 is a data broker.

18 “Data broker” means a commercial entity that, as a substantial
19 part of its business, collects, assembles, or maintains personally
20 identifiable information concerning an individual who is not a
21 customer or an employee of that entity in order to sell or trade the
22 information or provide third-party access to the information.

23 “Data minimization” means the practice of limiting the collection
24 and storage of personally identifiable information to what is
25 relevant and necessary to accomplish a specific purpose.

26 “Data protection impact assessment” means a study evaluating
27 the extent to which an information system protects the privacy and
28 security of personally identifiable information the system processes.

29 “Director” means the Director of the Division of Consumer
30 Affairs in the Department of Law and Public Safety.

31 “Division” means the Division of Consumer Affairs in the
32 Department of Law and Public Safety.

33 “High-risk automated decision system” means an automated
34 decision system that:

35 takes into account the novelty of the technology used and the
36 nature, scope, context, and purpose of the automated decision
37 system that poses a significant risk:

38 to the privacy or security of personally identifiable information
39 of consumers; or

40 results in or contributes to inaccurate, unfair, biased, or
41 discriminatory decisions impacting consumers;

42 makes decisions, or facilitates human decision making, based on
43 systematic and extensive evaluations of consumers, including
44 attempts to analyze or predict sensitive aspects of their lives, such
45 as their work performance, economic situation, health, personal
46 preferences, interests, behavior, location, or movements, that:

47 alter legal rights of consumers; or

48 otherwise significantly impact consumers;

1 involves the personally identifiable information of a significant
2 number of consumers regarding race, color, national origin,
3 political opinions, religion, union membership, genetic data,
4 biometric data, health, gender, gender identity, sexuality, sexual
5 orientation, criminal convictions, or arrests;

6 systematically monitors a large, publicly accessible physical
7 place; or

8 meets any other criteria established by the division in rules and
9 regulations issued pursuant to section 7 of P.L. , c. (C.)
10 (pending before the Legislature as this bill).

11 “High-risk information system” means an information system
12 that:

13 takes into account the novelty of the technology used and the
14 nature, scope, context, and purpose of the information system:

15 poses a significant risk to the privacy or security of personally
16 identifiable information of consumers;

17 involves the personally identifiable information of a significant
18 number of consumers regarding race, color, national origin,
19 political opinions, religion, union membership, genetic data,
20 biometric data, health, gender, gender identity, sexuality, sexual
21 orientation, criminal convictions, or arrests;

22 systematically monitors a large, publicly accessible physical
23 place; or

24 meets any other criteria established by the division pursuant to
25 P.L. , c. (C.) (pending before the Legislature as this bill).

26 “Information system” means a process, automated or manual,
27 that involves personally identifiable information, such as the
28 collection, recording, organization, structuring, storage, alteration,
29 retrieval, consultation, use, sharing, disclosure, dissemination,
30 combination, restriction, erasure, or destruction of personally
31 identifiable information and does not include automated decision
32 systems.

33 “Personally identifiable information” means any information
34 that, regardless of how the information is collected, inferred, or
35 obtained, is linked or reasonably linkable to a specific consumer or
36 consumer’s computer, mobile telecommunications service device,
37 or any other Internet-connected device.

38 “Store” means the actions of a covered entity to retain personally
39 identifiable information and includes actions to store, collect,
40 assemble, possess, control, or maintain information.

41 “Use” means the actions of a person, partnership, or corporation
42 in using information, including actions to use, process, or access
43 information.

44
45 3. a. Not later one year after the date of enactment of
46 P.L. , c. (C.) (pending before the Legislature as this bill), the
47 Director of the Division of Consumer Affairs in the Department of
48 Law and Public Safety shall require that a covered entity:

- 1 (1) conduct an automated decision system impact assessment of:
2 (a) the covered entity's existing high-risk automated decision
3 systems, as frequently as the director determines is necessary; and
4 (b) the covered entity's high-risk automated decision systems
5 developed since the previous automated decision system impact
6 assessment, if applicable, prior to its implementation;
7 (2) conduct a data protection impact assessment of:
8 (a) the covered entity's existing high-risk information systems,
9 as frequently as the director determines is necessary; and
10 (b) the covered entity's high-risk information systems developed
11 since the previous data protection impact assessment, if applicable,
12 prior to its implementation;
13 (3) conduct the impact assessments pursuant to paragraphs (1)
14 and (2) of subsection a. of this section in consultation with external
15 third parties, including independent auditors and independent
16 technology experts, if reasonably possible, as determined by the
17 director; and
18 (4) make record of any indication of racial or other bias, or any
19 threat to the security of a consumer's personally identifiable
20 information, found in the impact assessments required pursuant to
21 paragraphs (1) and (2) of subsection a. of this section, including any
22 measures taken by the covered entity to remedy these issues.
23 b. A covered entity may evaluate similar high-risk automated
24 decision systems and high-risk information systems that present
25 similar risks to the high-risk automated decision systems and high-
26 risk information systems assessed pursuant to paragraphs (1) and
27 (2) of subsection a. of this section in a single assessment for
28 purposes of comparison.
29 c. The impact assessments and information required pursuant
30 to this section shall be submitted to the director upon completion
31 and may be made public by the covered entity.
32
33 4. A waiver of the requirements of, or an agreement entered
34 into after the effective date of P.L. , c. (C.) (pending before
35 the Legislature as this bill), that does not comply with, the
36 provisions of section 3 of P.L. , c. (C.) (pending before the
37 Legislature as this bill) between a covered entity and a consumer
38 shall be void and unenforceable.
39
40 5. If the director determines, after reviewing the impact
41 assessments and information submitted pursuant to subsection c. of
42 section 3 of P.L. , c. (C.) (pending before the Legislature as
43 this bill), that an interest of the residents of the State has been or is
44 being threatened or adversely affected by a practice that violates
45 section 3 of P.L. , c. (C.) (pending before the Legislature as
46 this bill), the Attorney General of the State may institute civil action
47 on behalf of the residents of the State in an appropriate district court
48 of the United States to obtain appropriate relief.

1 threatened or adversely affected by a practice that violates the bill,
2 the Attorney General of the State may institute civil action on
3 behalf of the residents of the State in an appropriate district court of
4 the United States to obtain appropriate relief.

5 A violation of this bill's provisions is deemed an unlawful
6 practice and a violation of the consumer fraud act, which includes a
7 penalty of not more than \$10,000 for the first offense and not more
8 than \$20,000 for the second and each subsequent offense.