116TH CONGRESS
1ST SESSION

S. 1108

To direct the Federal Trade Commission to require entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments.

IN THE SENATE OF THE UNITED STATES

APRIL 10, 2019

Mr. Wyden (for himself and Mr. Booker) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To direct the Federal Trade Commission to require entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Algorithmic Accountability Act of 2019”.

SEC. 2. DEFINITIONS.

In this Act:
(1) AUTOMATED DECISION SYSTEM.—The term “automated decision system” means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers.

(2) AUTOMATED DECISION SYSTEM IMPACT ASSESSMENT.—The term “automated decision system impact assessment” means a study evaluating an automated decision system and the automated decision system’s development process, including the design and training data of the automated decision system, for impacts on accuracy, fairness, bias, discrimination, privacy, and security that includes, at a minimum—

(A) a detailed description of the automated decision system, its design, its training, data, and its purpose;

(B) an assessment of the relative benefits and costs of the automated decision system in light of its purpose, taking into account relevant factors, including—

(i) data minimization practices;
(ii) the duration for which personal
information and the results of the auto-
mated decision system are stored;

(iii) what information about the auto-
mated decision system is available to con-
sumers;

(iv) the extent to which consumers
have access to the results of the automated
decision system and may correct or object
to its results; and

(v) the recipients of the results of the
automated decision system;

(C) an assessment of the risks posed by
the automated decision system to the privacy or
security of personal information of consumers
and the risks that the automated decision sys-
tem may result in or contribute to inaccurate,
unfair, biased, or discriminatory decisions im-
pacting consumers; and

(D) the measures the covered entity will
employ to minimize the risks described in sub-
paragraph (C), including technological and
physical safeguards.

(3) COMMISSION.—The term “Commission”
means the Federal Trade Commission.
(4) **CONSUMER.**—The term “consumer” means an individual.

(5) **COVERED ENTITY.**—The term “covered entity” means any person, partnership, or corporation over which the Commission has jurisdiction under section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)) that—

(A) had greater than $50,000,000 in average annual gross receipts for the 3-taxable-year period preceding the most recent fiscal year, as determined in accordance with paragraphs (2) and (3) of section 448(c) of the Internal Revenue Code of 1986;

(B) possesses or controls personal information on more than—

(i) 1,000,000 consumers; or

(ii) 1,000,000 consumer devices;

(C) is substantially owned, operated, or controlled by a person, partnership, or corporation that meets the requirements under subparagraph (A) or (B); or

(D) is a data broker or other commercial entity that, as a substantial part of its business, collects, assembles, or maintains personal information concerning an individual who is not a
customer or an employee of that entity in order
to sell or trade the information or provide third-
party access to the information.

(6) DATA PROTECTION IMPACT ASSESSMENT.—
The term “data protection impact assessment”
means a study evaluating the extent to which an in-
formation system protects the privacy and security
of personal information the system processes.

(7) HIGH-RISK AUTOMATED DECISION SYS-
TEM.—The term “high-risk automated decision sys-
stem” means an automated decision system that—

(A) taking into account the novelty of the
technology used and the nature, scope, context,
and purpose of the automated decision system,
poses a significant risk—

(i) to the privacy or security of per-
sonal information of consumers; or

(ii) of resulting in or contributing to
inaccurate, unfair, biased, or discrimina-
tory decisions impacting consumers;

(B) makes decisions, or facilitates human
decision making, based on systematic and ex-
tensive evaluations of consumers, including at-
ttempts to analyze or predict sensitive aspects of
their lives, such as their work performance, eco-
nominal situation, health, personal preferences, interests, behavior, location, or movements, that—

(i) alter legal rights of consumers; or

(ii) otherwise significantly impact consumers;

(C) involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests;

(D) systematically monitors a large, publicly accessible physical place; or

(E) meets any other criteria established by the Commission in regulations issued under section 3(b)(1).

(8) HIGH-RISK INFORMATION SYSTEM.—The term “high-risk information system” means an information system that—

(A) taking into account the novelty of the technology used and the nature, scope, context, and purpose of the information system, poses a
significant risk to the privacy or security of personal information of consumers;

(B) involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests;

(C) systematically monitors a large, publicly accessible physical place; or

(D) meets any other criteria established by the Commission in regulations issued under section 3(b)(1).

(9) INFORMATION SYSTEM.—The term “information system”—

(A) means a process, automated or not, that involves personal information, such as the collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, sharing, disclosure, dissemination, combination, restriction, erasure, or destruction of personal information; and

(B) does not include automated decision systems.
(10) **PERSONAL INFORMATION.**—The term “personal information” means any information, regardless of how the information is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device.

(11) **STORE.**—The term “store”—

(A) means the actions of a person, partnership, or corporation to retain information; and

(B) includes actions to store, collect, assemble, possess, control, or maintain information.

(12) **USE.**—The term “use” means the actions of a person, partnership, or corporation in using information, including actions to use, process, or access information.

**SEC. 3. DATA PROTECTION AUTHORITY.**

(a) **ACTS PROHIBITED.**—It is unlawful for any covered entity to—

(1) violate a regulation promulgated under subsection (b); or

(2) knowingly provide substantial assistance to any person, partnership, or corporation whose actions violate subsection (b).

(b) **REGULATIONS.**—
(1) IN GENERAL.—Not later than 2 years after the date of enactment of this section, the Commission shall promulgate regulations, in accordance with section 553 of title 5, United States Code, that—

(A) require each covered entity to conduct automated decision system impact assessments of—

(i) existing high-risk automated decision systems, as frequently as the Commission determines is necessary; and

(ii) new high-risk automated decision systems, prior to implementation,

provided that a covered entity may evaluate similar high-risk automated decision systems that present similar risks in a single assessment;

(B) require each covered entity to conduct data protection impact assessments of—

(i) existing high-risk information systems, as frequently as the Commission determines is necessary; and

(ii) new high-risk information systems, prior to implementation,
provided that a covered entity may evaluate
similar high-risk information systems that
present similar risks in a single assessment;

(C) require each covered entity to conduct
the impact assessments under subparagraphs
(A) and (B), if reasonably possible, in consulta-
tion with external third parties, including inde-
pendent auditors and independent technology
experts; and

(D) require each covered entity to reason-
ably address in a timely manner the results of
the impact assessments under subparagraphs
(A) and (B).

(2) OPTIONAL PUBLICATION OF IMPACT AS-
SESSMENTS.—The impact assessments under sub-
paragraphs (A) and (B) may be made public by the
covered entity at its sole discretion.

(c) PREEMPTION OF PRIVATE CONTRACTS.—It shall
be unlawful for any covered entity to commit the acts pro-
hibited in subsection (a), regardless of specific agreements
between entities or consumers.

(d) ENFORCEMENT BY THE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of subsection (a) shall be treated
as a violation of a rule defining an unfair or decep-
tive act or practice under section 18(a)(1)(B) of the
57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—The Commission shall
enforce this section in the same manner, by the
same means, and with the same jurisdiction,
powers, and duties as though all applicable
terms and provisions of the Federal Trade
Commission Act (15 U.S.C. 41 et seq.) were in-
corporated into and made a part of this section.

(B) PRIVILEGES AND IMMUNITIES.—Any
person who violates subsection (a) shall be sub-
ject to the penalties and entitled to the privi-
leges and immunities provided in the Federal

(C) AUTHORITY PRESERVED.—Nothing in
this section shall be construed to limit the au-
thority of the Commission under any other pro-
vision of law.

(e) ENFORCEMENT BY STATES.—

(1) IN GENERAL.—If the attorney general of a
State has reason to believe that an interest of the
residents of the State has been or is being threat-
ened or adversely affected by a practice that violates
subsection (a), the attorney general of the State may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to obtain appropriate relief.

(2) Rights of Commission.—

(A) Notice to Commission.—

(i) In general.—Except as provided in clause (iii), the attorney general of a State, before initiating a civil action under paragraph (1), shall provide written notification to the Commission that the attorney general intends to bring such civil action.

(ii) Contents.—The notification required under clause (i) shall include a copy of the complaint to be filed to initiate the civil action.

(iii) Exception.—If it is not feasible for the attorney general of a State to provide the notification required under clause (i) before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately upon instituting the civil action.
(B) Intervention by Commission.—The Commission may—

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening—

(I) be heard on all matters arising in the civil action; and

(II) file petitions for appeal of a decision in the civil action.

(3) Investigatory Powers.—Nothing in this subsection may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(4) Venue; Service of Process.—

(A) Venue.—Any action brought under paragraph (1) may be brought in—

(i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or
(ii) another court of competent juris-
diction.

(B) SERVICE OF PROCESS.—In an action
brought under paragraph (1), process may be
served in any district in which—

(i) the defendant is an inhabitant,

(ii) venue is proper under section

1391 of title 28, United States Code.

(5) ACTIONS BY OTHER STATE OFFICIALS.—

(A) IN GENERAL.—In addition to a civil
action brought by an attorney general under
paragraph (1), any other officer of a State who
is authorized by the State to do so may bring
a civil action under paragraph (1), subject to
the same requirements and limitations that
apply under this subsection to civil actions
brought by attorneys general.

(B) SAVINGS PROVISION.—Nothing in this
subsection may be construed to prohibit an au-
thorized official of a State from initiating or
continuing any proceeding in a court of the
State for a violation of any civil or criminal law
of the State.
SEC. 4. NO PREEMPTION.

Nothing in this Act may be construed to preempt any State law.