A BILL

To require the Federal Trade Commission to promulgate regulations related to sensitive personal information, and for other purposes.

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 “Information Transparency & Personal Data Control Act”.

SEC. 2. SENSE OF CONGRESS.

It is the Sense of Congress that—

(1) the United States must develop a balanced, high-standard digital privacy framework that complements global standards;

(2) a key element of this framework is a strong national standard that combats anti-consumer practices;

(3) it is critical that the Federal Government provide guidance on the collection, processing, disclosure, transmission and storage of sensitive data;

(4) it is important to provide the Nation with fair and thoughtful digital consumer rights with respect to such data;

(5) it is important to ensure that enforcement authorities have the resources needed to protect consumers from unlawful and deceptive acts of practices in the data privacy and security space; and

(6) individuals have a right to—

(A) exercise control over the personal data companies collect from them and how they use it;

(B) easily understandable and accessible information about privacy and security practices;

(C) expect that companies will collect, use, and disclose personal data in ways that are consistent
with the context in which consumers provide the
data;

(D) secure and responsible handling of sensitive
personal information;

(E) access and correct persona data in usable
formats, in a manner that is appropriate to
sensitivity of the data and the risk of adverse
consequences to consumers if the data is inaccurate;
and

(F) reasonable limits on the personal data that
companies collect and retain.

SEC. 3. REQUIREMENTS FOR SENSITIVE PERSONAL INFORMATION.

(a) REGULATIONS.—Not later than 18 months after the date of
enactment of this Act, the Federal Trade Commission shall
promulgate regulations under section 553 of title 5, United States
Code, to require, except as provided in subsection (b), controllers,
processors, and third parties to make available to the public
involving the collection, transmission, storage, processing, sale,
sharing of sensitive personal information, or other use of sensitive
personal information from persons operating in or persons located
in the United States when the sensitive personal information is
collected, transmitted, stored, processed, sold or shared to meet the
following requirements:

(1) AFFIRMATIVE, EXPRESS, AND OPT-IN CONSENT.—

(A) Any controller shall provide users whose
personal information is collected, transmitted, stored,
process, sold, or otherwise shared with notice through a
privacy and data use policy of a specific request to collect,
transmit, sell, share or otherwise disclose their sensitive
personal information and require that users provide
affirmative, express consent to any functionality that
involves the collection, sale, sharing, or other disclosure of
sensitive personal information, including sharing sensitive
personal information with third parties, if the sensitive
personal information is to be used by the third party for
purposes other than the purposes outlined in the notice.

(B) The documented instruction from a controller to
a processor or third party shall adhere to the limits of the
consent granted in subparagraph (A), and processors and
third parties shall not use or disclose the sensitive personal information for any other purposes or in any way that exceeds the limits of the consent granted in subparagraph (A).

(D) Controllers and processors shall not be liable for the failure of another processor or third party to adhere to the limits of an opt-in consent granted under subparagraph (A).

(2) PRIVACY AND DATA USE POLICY.—Controllers, processors, and third parties shall publicly maintain an up-to-date, transparent privacy, security, and data use policy that meets general requirements, including that such policy, presented in the context where it applies—

(A) is concise, intelligible, and uses plain language;

(B) is clear and conspicuous consistent with the guidelines of the Federal Trade Commission;

(C) uses visualizations, where appropriate to make complex information understandable by the ordinary user; and

(D) is provided free of charge.

(3) ADDITIONAL REQUIREMENTS FOR PRIVACY AND DATA USE POLICY.—The privacy, security, and data use policy required under paragraph (2) shall include the following:

(A) Identity and contact information of the entity collecting or processing the sensitive personal information.

(B) The purpose or use for collecting, storing, processing, selling, sharing, or otherwise using the sensitive personal information.

(C) Categories of third parties with whom the sensitive personal information will be shared and for what general purposes.

(D) The process by which individuals may withdraw consent to the collecting, storing, processing,
selling, sharing, or other use of the sensitive personal
information, including sharing with third parties.

(E) How a user, controller, or processor can view or
obtain the sensitive personal information that they have
received or provided to a controller or processor, including
whether it can be exported to other web-based platforms.

(F) The categories of sensitive personal information
that is collected by the controller or processor and shared
with processors or third parties.

(G) How sensitive personal information is protected
from unauthorized access or acquisition.

(4) OPT-OUT CONSENT.—

(A) For any collection, transmission, storage,
processing, selling, sharing, or other use of non-sensitive
personal information, including sharing with third parties,
controllers shall provide users with the ability to opt out at
any time.

(B) Controllers shall honor an opt out request from
a user under subparagraph (A) to the extent of its role in
any collection, transmission, storage, processing, selling,
sharing, or other use of non-sensitive personal information
and shall communicate an opt-out request to the relevant
processor or third party with which the controller has
shared information regarding that user.

(C) Processors or third parties receiving an opt out
pursuant to subparagraph (A) and (B) shall comply with
such opt out to the extent of their role in any collection,
transmission, storage, processing, selling, sharing, or other
use of non-sensitive personal information.

(D) Any controller that communicates an opt out
from a user as required by subparagraph (B) shall not be
liable for the failure of a service provider or third party to
comply with such opt out.

(5) Relationship Between Controller and Processor

(A) Processing by a processor must be governed
by a contract between the controller and the
processor that is binding on both parties and
that sets the processor to processes the
personal data only on documented
instructions from the controller.

(B) Processors shall share sensitive personal
information with a subcontractor only for
purposes of providing services and only
after first providing the controller with an
opportunity to object.

(C) In no event may any contract or documented
instructions relieve a controller or a
processor from the obligations and liabilities
imposed on them by this Act.

(6) PRIVACY AUDITS.—

(A) IN GENERAL.—Except as provided in
paragraphs (C) and (D), at least once every 2 years,
each controller, processor, or third party that has collected,
transmitted, stored, processed, selling, shared, or otherwise
used sensitive personal information shall—

(i) obtain a privacy audit from a qualified,
objective, independent third party; and

(ii) shall make publicly available whether or
not the privacy audit found the controller,
processor, or third party compliant.

(B) AUDIT REQUIREMENTS.—Each such audit
shall—

(i) set forth the privacy, security, and data
use controls that the controller, processor, or
third party has implemented and maintained
during the reporting period;

(ii) describe whether such controls are
appropriate to the size and complexity of the
controller, processor, or third party, the
nature and scope of the activities of the
controller, processor, or third party, and the
nature of the sensitive personal information
or behavioral data collected by the
controller, processor, or third party;
(iii) certify whether the privacy and security controls operate with sufficient effectiveness to provide reasonable assurance to protect the privacy and security of sensitive personal information or behavioral data, including with respect to data shared with third parties, and that the controls have so operated throughout the reporting period;

(iv) be prepared and completed within 60 days after a substantial change to the controller’s privacy and data use policy described in paragraph (2); and

(v) be provided—

(I) to the Federal Trade Commission; and

(II) to any attorney general of a State, or other authorized State officer, within 10 days of receiving written request by the such attorney general, or other authorized State officer where such officer has presented to the controller, processor, or third party allegations that a violation of his Act or any regulation issued under this Act has been committed by the controller, processor, or third party.

(C) SMALL BUSINESS AUDIT EXEMPTION.—The audit requirements described in this paragraph shall not apply to controllers who collect, store, process, sell, share, or otherwise use sensitive personal information relating to 250,000 or fewer individuals per year.

(D) NON-SENSITIVE PERSONAL INFORMATION EXEMPTION.—The audit requirements set forth above shall not apply to controllers, processors or third parties who do not collect, store, process, sell, share, or otherwise use sensitive personal information.

(E) RULES THAT DO NOT INCENTIVIZE SELLING INFORMATION.—The Commission shall promulgate rules
regarding qualifications and requirements of third-party
auditors such as a duty to conduct an independent
assessment that does not incentivize the auditor to sell
under the guise of a potential violation by the controller
products or services when there is not a violation of the
Act.

(b) EXEMPTIONS.—

(1) NECESSARY OPERATIONS AND SECURITY PURPOSES.—
Subsection (a) shall not apply to the processing, transmission,
collecting, storing, sharing, selling of sensitive and non-sensitive
personal information for the following purposes:

(A) Preventing or detecting fraud, identity theft,
unauthorized transactions, theft, shoplifting, or criminal
activity including financial crimes and money laundering.

(B) The use of such information to identify errors
that impair functionality or otherwise enhancing or
maintaining the availability of the services or information
systems of the controller for authorized access and use.

(C) Protecting the vital interests of the consumer or
another natural person.

(D) Responding in good faith to valid legal process
or providing information as otherwise required or
authorized by law.

(E) Monitoring or enforcing agreements between
the Controller, processor, or third party and an individual,
including but not limited to, terms of service, terms of use,
user agreements, or agreements concerning monitoring
criminal activity.

(F) Protecting the property, services, or information
systems of the controller, processor, or third party against
unauthorized access or use.

(G) Advancing a substantial public interest,
including archival purposes, scientific or historical
research, and public health, if such processing does not
create a significant risk of harm to consumers.
(H) Uses authorized by the Fair Credit Reporting Act or used by a commercial credit reporting agency.

(I) Completing the transaction for which the personal information was collected, provide a good or service requested by the consumer that is reasonably anticipated within the context of a business’ ongoing relationship with the consumer, bill or collect for such good or service or otherwise perform a contract between the controller and a consumer.

(J) Complying with other Federal, State, and local law.

(K) Conducting product recalls and servicing warranties.

(2) REASONABLE EXPECTATION OF USERS.— The regulations promulgated pursuant to subsection (a) with respect to the requirement to provide opt-in consent shall not apply to the processing, transmission, storage, selling, sharing, or collection of sensitive personal information in which such processing does not deviate from purposes consistent with a controller’s relationship with users as understood by the reasonable use, including but not limited to—

(A) carrying out the term of a contract or service agreement, including elements of a customer loyalty program, with a user;

(B) accepting and processing a payment from a user;

(C) completing a transaction with a user such as through delivering a good or service even if such delivery is made by a processor or third party;

(D) marking goods or services to a user as long as the user is provided with the ability to opt out of such marketing;

(E) taking steps to continue or extend an existing business relationship with a user, or inviting a new user to participate in a customer promotion, benefit or loyalty program, as long as the user is provided with the ability to opt out;
(F) conduct internal research to improve, repair, or develop products, services, or technology; or

(G) municipal governments.

SEC. 4. APPLICATION AND ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) COMMON CARRIERS.—Notwithstanding the limitations in the Federal Trade Commission Act (15 U.S.C. 15 41 et seq.) on Commission authority with respect to common carriers, this Act applies, according to its terms, to common carriers subject to the Communications Act of (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto. The Federal Trade Commission shall be the only Federal agency with authority to enforce such common carriers’ privacy practices.

(b) ENFORCEMENT.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—Except as provided in subsection (a), the Federal Trade Commission shall enforce this Act and the regulations promulgated under this Act 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 incorporated into and made a part of this Act. Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(c) CONSTRUCTION.—Nothing in this Act shall be construed to limit the authority of the Federal Trade Commission under any other provision of law.

(d) OPPORTUNITY TO COMPLY.—The Commission shall notify a controller of alleged violations and provide them with 30 days to cure a non-wilful violations of this Act before the Commission shall commence and enforcement action.
SEC. 5. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) RIGHT OF ACTION.—Except as provided in subsection (e), the attorney general of a State, alleging a violation of this Act or any regulation issued under this Act that affects or may affect such State or its residents may bring an action on behalf of the residents of the State in any United States district court for the district in which the defendant is found, resides, or transacts business, or wherever venue is proper under section 1391 of title 28, United States Code, to obtain appropriate injunctive relief.

(b) NOTICE TO COMMISSION REQUIRED.—A State shall provide prior written notice to the Federal Trade Commission of any civil action under subsection (a) together with a copy of its complaint, except that if it is not feasible for the State to provide such prior notice, the State shall provide such notice immediately upon instituting such action.

(c) INTERVENTION BY THE COMMISSION.—The Commission may intervene in such civil action and upon intervening—

(1) be heard on all matters arising in such civil action; and

(2) file petitions for appeal of a decision in such civil action.

(d) CONSTRUCTION.—Nothing in this section shall be construed—

(1) to prevent the attorney general of a State, or other authorized State officer, from exercising the powers conferred on the attorney general, or other authorized State officer, by the laws of such State; or

(2) to prohibit the attorney general of a State, or other authorized State officer, from proceeding in State or Federal court on the basis of an alleged violation of any civil or criminal statute of that State.

(e) LIMITATION.—

(1) NO SEPARATE ACTION.—An action may not be brought under subsection (a) if the same alleged violation is the subject of a pending action by the Commission or the United States.

(2) EXCLUSIVE PERIOD TO ACT BY COMMISSION.—An action—
(A) may not be brought under subsection (a) until the expiration of the 60-day period that begins on the date on which a violation is discovered by the Commission or the date on which the Commission is notified of the violation; and

(B) may only be brought under subsection (a) if the Commission does not bring an action related to the violation during such period.

(f) OPPORTUNITY TO COMPLY.—Prior to bringing any action under this section, the state attorney general shall notify a controller of alleged violations and provide them with 30 days to cure a non-wilful violation of this Act before commencing an enforcement action.

SEC. 6. PRIVACY AND DATA SECURITY EMPLOYEES AND FUNDING FOR THE COMMISSION.

(a) EMPLOYMENT AUTHORITY.—The Commission shall hire 500 new full-time employees to focus on privacy and data security, 50 of which shall have technology expertise.

(b) ADDITIONAL FUNDING FOR PRIVACY AND DATA SECURITY.—There is authorized to be appropriated to the Commission $350,000,000 for issues related to privacy and data security.

SEC. 7. DEFINITIONS.

In this Act the following definitions apply:

(1) CALL DETAIL RECORD.—The term “call detail record” —

(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call;

(B) does not include—

(i) the contents (as defined in section (8) of title 18, United States Code) of any communication;
(ii) the name, address, or financial
information of a subscriber or customer;

(iii) cell site location or global positioning
system information; or

(iv) business customers.

(2) CLEAR AND PROMINENT.—The term “clear and
prominent” means in any communication medium, the required
disclosure is—

(A) of a type, size, and location sufficiently
noticeable for an ordinary consumer to read and
comprehend the communication;

(B) provided in a manner such that an ordinary
consumer is able to read and comprehend the
communication;

(C) is presented in an understandable language and
syntax;

(D) includes nothing contrary to, inconsistent with,
or that mitigates any statement contained within the
disclosure or within any document linked to or
referred to therein; and

(E) includes an option that is compliant with
applicable obligations of the controller under title
III of the Americans with Disabilities Act of 1990
(42 U.S.C. 12181 et seq.).

(3) COLLECTION.— The term “collection” means buying,
renting, gathering, obtaining, receiving, or accessing any sensitive
data of an individual by any means.

(4) COMMISSION.—The term “Commission” means the
Federal Trade Commission.

(5) CONTROLLER.—The term “controller” means a person
that, on its own or jointly with other entities, determines the
purposes and means of processing sensitive personal information.

(6) DE-IDENTIFIED DATA.—The term “de-identified data”
means information held that—
(A) does not identify, and is not linked or reasonably linkable to, an individual or device;

(B) does not contain a persistent identifier or other information that could readily be used to de-identify the individual to whom, or the device to which, the identifier or information pertains;

(C) is subject to a public commitment by the entity;

(D) to refrain from attempting to use such information to identify any individual or device;

(E) to adopt technical and organizational measures to ensure that such information is not linked to any individual or device; and

(F) is not disclosed by the covered entity to any other party unless the disclosure is subject to a contractually or other legally binding requirement.

(7) EMPLOYEE DATA.—The term “employee data” means—

(A) information relating to an individual collected in the course of the individual acting as a job applicant to, or employee (regardless of whether such employee is paid or unpaid, or employed on a temporary basis), owner, director, officer, staff member, trainee, vendor, visitor, volunteer, intern, or contractor;

(B) business contact information of an individual, including the individual’s name, position or title, business telephone number, business address, business email address, qualifications, and other similar information that is provided by an individual who is acting in a professional capacity, provided that such information is collected, processed, or transferred solely for purposes related to such individuals’ professional activities; or

(C) emergency contact information collected by a covered entity that relates to an individual who is acting in a role described in subparagraph (A).
(8) PROCESSOR.—The term “processor” means a person that processes data on behalf of a controller or another processor according to and for the purposes set forth in the documented instructions. If a person processes data on its own behalf or for its own purposes then that person is not a processor with respect to that data but is instead a controller. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the controller’s documented instructions and the context in which personal data is to be processed. A processor shall only remain a processor to the extent that it continues to process data for the sole purposes set forth in the documented instructions of the controller and adheres to those instructions and the limitations in the controller’s privacy policy as communicated to the processor with respect to a specific processing of personal information.

(9) SENSITIVE PERSONAL INFORMATION.—

(A) The term “sensitive personal information” means information relating to an identified or identifiable individual that is—

(i) financial account numbers;

(ii) health information;

(iii) genetic data;

(iv) any information pertaining to children under 13 years of age;

(v) Social Security numbers;

(vi) unique government-issued identifiers;

(vii) authentication credentials for a financial account, such as a username and password;

(viii) precise geolocation information;

(ix) content of a personal wire communication, oral communication, or electronic communication such as e-mail or direct messaging with respect to any entity.
that is not the intended recipient of the communication;

(x) call detail records for calls conducted in a personal and not a business capacity;

(xi) biometric information;

(xii) sexual orientation, gender identity, or intersex status;

(xiii) citizenship or immigration status;

(xiv) mental or physical health diagnosis;

(xv) religious beliefs; or

(xvi) web browsing history, application usage history, and the functional equivalent of either that is data described in this subparagraph that is not aggregated data.

(B) The term “sensitive personal information” does not include—

(i) de-identified information (or the measurement, analysis or process utilized to transforming personal data so that it is not directly relatable to an identified or identifiable consumer);

(ii) information related to employment, including any employee data;

(iii) personal information reflecting a written or verbal communication or a transaction between a controller and the user, where the user is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the controller occur solely within the context of the controller conducting due diligence regarding, or providing or receiving a product or service
to or from such company, partnership, sole
proprietorship, non-profit, or government
agency; or

(iv) publicly available information.

(10) STATE.—The term “State” means each State of the
United States, the District of Columbia, and each commonwealth,
territory, or possession of the United States.

(11) THIRD PARTY.—The term “third party” means an
individual or entity that uses or receives sensitive personal
information obtained by or on behalf of a controller, other than—

(A) a service provider of a controller to whom the
controller discloses the consumer’s sensitive
personal information for an operational purpose
subject to section 3(a)(1)(B) of this Act; and

(B) any entity that uses sensitive personal
information only as reasonably necessary—

(i) to comply with applicable law,
regulation, or legal process;

(ii) to enforce the terms of use of a
controller;

(iii) to detect, prevent, or mitigate fraud or
security vulnerabilities; or

(iv) does not determine the purposes and
means of processing sensitive personal
information.

(12) TRANSFER.—The term “transfer” means to disclose,
release, share, disseminate, make available, or license in writing,
electronically or by any other means, for consideration of any kind
for a commercial purpose.

SEC. 8. RULES OF CONSTRUCTION.

(a) FEDERAL ACQUISITION.—Nothing in this Act may be
construed to preclude the acquisition by the Federal Government
of—

(1) the contents of a wire or electronic communication
pursuant to other lawful authorities, including the authorities under
chapter 119 of title 18, United States Code (commonly known as the “Wiretap Act”), the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this Act; or

(2) records or other information relating to a subscriber or customer of any electronic communication service or remote computing service (not including the content of such communications) pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119 of title 18, United States Code (commonly known as the “Wiretap Act”), or any other provision of Federal law not specifically amended by this Act.


SEC. 9. NATIONAL STANDARD.

(a) RELATIONSHIP TO STATE LAW.—No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or associated activities of covered entities.

(b) NONPREEMPTION.—Subsection (a) shall not be construed to—

(1) preempt State laws that directly establish requirements for the notification of consumers in the event of a data breach;

(2) preempt State laws that directly establish requirements regarding biometric laws;

(3) preempt State laws regarding wiretapping laws; or

(4) preempt State laws like the Public Records Act.

SEC. 10. EFFECTIVE DATE.

This Act shall take effect 180 days after the date of the enactment of this Act.