

HB3041



104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

HB3041

Introduced 2/6/2025, by Rep. Abdelnasser Rashid

SYNOPSIS AS INTRODUCED:

New Act

Creates the Illinois Data Privacy and Protection Act. Provides that a covered entity (any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data) may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate. Provides that a covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures concerning the collection, processing, and transferring of covered data. Contains provisions concerning retaliation; transparency; individual data rights; consent; data protection for children and minors; civil rights; data security; small business protections; executive responsibility; service providers and third parties; enforcement; severability; and rulemaking. Effective 180 days after becoming law.

LRB104 08482 SPS 18534 b

A BILL FOR

1 AN ACT concerning business.

2 **Be it enacted by the People of the State of Illinois,**
3 **represented in the General Assembly:**

4 Section 1. Short title. This Act may be cited as the
5 Illinois Data Privacy and Protection Act.

6 Section 5. Definitions. As used in this Act:

7 "Affirmative express consent" means an affirmative act by
8 an individual that clearly communicates the individual's
9 freely given, specific, and unambiguous authorization for an
10 act or practice after having been informed, in response to a
11 specific request from a covered entity, provided:

12 (1) The request is provided to the individual in a
13 clear and conspicuous standalone disclosure made through
14 the primary medium used to offer the covered entity's
15 product or service, or only if the product or service is
16 not offered in a medium that permits the making of the
17 request under this paragraph, another medium regularly
18 used in conjunction with the covered entity's product or
19 service.

20 (2) The request includes a description of the
21 processing purpose for which the individual's consent is
22 sought and:

23 (A) clearly states the specific categories of

1 covered data that the covered entity shall collect,
2 process, and transfer necessary to effectuate the
3 processing purpose; and

4 (B) includes a prominent heading and is written in
5 easy-to-understand language that would enable a
6 reasonable individual to identify and understand the
7 processing purpose for which consent is sought and the
8 covered data to be collected, processed, or
9 transferred by the covered entity for such processing
10 purpose.

11 (3) The request clearly explains the individual's
12 applicable rights related to consent.

13 (4) The request is made in a manner reasonably
14 accessible to and usable by individuals with disabilities.

15 (5) The request is made available to the individual in
16 each covered language in which the covered entity provides
17 a product or service for which authorization is sought.

18 (6) The option to refuse consent shall be at least as
19 prominent as the option to accept, and the option to
20 refuse consent shall take the same number of steps or
21 fewer as the option to accept.

22 (7) Processing or transferring any covered data
23 collected pursuant to affirmative express consent for a
24 different processing purpose than that for which
25 affirmative express consent was obtained shall require
26 affirmative express consent for the subsequent processing

purpose.

(8) affirmative express consent to an act or practice is not inferred from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(9) Affirmative express consent is not obtained or attempted to be obtained through:

(A) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(B) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision-making, or choice to provide such consent or any covered data.

"Authentication" means the process of verifying an individual or entity for security purposes.

"Biometric information" means any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual. including, but is not limited to, fingerprints, voice prints, iris or retina scans, facial or hand mapping, geometry, or templates; or gait or other unique body movements. "Biometric information" does not include a digital or physical photograph, an audio or video recording, or data generated from a digital or physical

1 photograph, or an audio or video recording, that cannot be
2 used, alone or in combination with other information, to
3 identify an individual.

4 "Collect" and "collection" means buying, renting,
5 gathering, obtaining, receiving, accessing, or otherwise
6 acquiring covered data by any means.

7 "Control" means, with respect to an entity:

8 (1) ownership of, or the power to vote, more than 50%
9 of the outstanding shares of any class of voting security
10 of the entity;

11 (2) control over the election of a majority of the
12 directors of the entity (or of individuals exercising
13 similar functions); or

14 (3) the power to exercise a controlling influence over
15 the management of the entity.

16 "Covered algorithm" means a computational process that
17 uses machine learning, natural language processing, artificial
18 intelligence techniques, or other computational processing
19 techniques of similar or greater complexity and that makes a
20 decision or facilitates human decision-making with respect to
21 covered data, including to determine the provision of products
22 or services or to rank, order, promote, recommend, amplify, or
23 similarly determine the delivery or display of information to
24 an individual.

25 "Covered data" means information, including derived data
26 and unique identifiers, that identifies or is linked or

1 reasonably linkable, alone or in combination with other
2 information, to an individual or a device that identifies or
3 is linked or reasonably linkable to an individual; provided,
4 however, that "covered data" does not include

- 5 (1) de-identified data;
- 6 (2) employee data; or
- 7 (3) publicly available information.

8 "Covered entity" means any entity or any person, other
9 than an individual acting in a non-commercial context, that
10 alone or jointly with others determines the purposes and means
11 of collecting, processing, or transferring covered data.
12 "Covered entity" includes any entity or person that controls,
13 is controlled by, or is under common control with the covered
14 entity. An entity shall not be considered to be a covered
15 entity for purposes of this Act in so far as the entity is
16 acting as a service provider. "Covered entity" does not
17 include:

18 (1) a federal, State, tribal, territorial, or local
19 government entity such as a body, authority, board,
20 bureau, commission, district, agency, or political
21 subdivision of the federal government or a State, tribal,
22 territorial, or local government;

23 (2) a person or an entity that is collecting,
24 processing, or transferring covered data on behalf of a
25 federal, State, tribal, territorial, or local government
26 entity, in so far as such person or entity is acting as a

1 service provider to the government entity; or

2 (3) an entity that serves as a congressionally
3 designated nonprofit, national resource center, and
4 clearinghouse to provide assistance to victims, families,
5 child-serving professionals, and the general public on
6 missing and exploited children issues.

7 "Covered high-impact social media company" means a covered
8 entity that provides any Internet-accessible platform where:

9 (1) such covered entity generates \$3,000,000,000 or
10 more in annual revenue;

11 (2) such platform has 300,000,000 or more monthly
12 active users for not fewer than 3 of the preceding 12
13 months on the online product or service of such covered
14 entity; and

15 (3) such platform constitutes an online product or
16 service that is primarily used by users to access or
17 share, user-generated content.

18 "Covered language" means the 10 languages with the most
19 speakers in the United States, according to the most recent
20 decennial census.

21 "Covered minor" means an individual under the age of 17.

22 "Data broker" means a covered entity whose principal
23 source of revenue is derived from processing or transferring
24 covered data that the covered entity did not collect directly
25 from the individuals linked or linkable to the covered data;
26 and does not include a covered entity insofar as such entity

1 processes employee data collected by and received from a third
2 party concerning any individual who is an employee of the
3 third party for the sole purpose of such third party providing
4 benefits to the employee. An entity may not be considered to be
5 a data broker for purposes of this Act if the entity is acting
6 as a service provider. For purposes of this definition,
7 "principal source of revenue" means, for the prior 12-month
8 period, either:

9 (1) more than 50% of all revenue of the covered
10 entity; or

11 (2) obtaining revenue from processing or transferring
12 the covered data of more than 5,000,000 individuals that
13 the covered entity did not collect directly from the
14 individuals linked or linkable to the covered data.

15 "De-identified data" means information that does not
16 identify and is not linked or reasonably linkable to a
17 distinct individual or a device, regardless of whether the
18 information is aggregated, and if the covered entity or
19 service provider:

20 (1) takes technical measures that ensure that the
21 information cannot, at any point, be used to re-identify
22 any individual or device that identifies or is linked or
23 reasonably linkable to an individual;

24 (2) publicly commits in a clear and conspicuous
25 manner:

26 (A) to process and transfer the information solely

1 in a de-identified form without any reasonable means
2 for re-identification; and

3 (B) to not attempt to re-identify the information
4 with any individual or device that identifies or is
5 linked or reasonably linkable to an individual; and

6 (3) contractually obligates any person or entity that
7 receives the information from the covered entity or
8 service provider:

9 (A) to comply with all of the provisions of this
10 paragraph with respect to the information; and

11 (B) to require that such contractual obligations
12 be included contractually in all subsequent instances
13 for which the data may be received.

14 "Derived data" means covered data that is created by the
15 derivation of information, data, assumptions, correlations,
16 inferences, predictions, or conclusions from facts, evidence,
17 or another source of information or data about an individual
18 or an individual's device.

19 "Device" means any electronic equipment capable of
20 collecting, processing, or transferring covered data that is
21 used by one or more individuals.

22 "Employee" means an individual who is an employee,
23 director, officer, staff member, individual working as an
24 independent contractor that is not a service provider,
25 trainee, volunteer, or intern of an employer, regardless of
26 whether such individual is paid, unpaid, or employed on a

1 temporary basis.

2 "Employee data" means:

3 (1) information relating to a job applicant collected
4 by a covered entity acting as a prospective employer of
5 such job applicant in the course of the application, or
6 hiring process, if such information is collected,
7 processed, or transferred by the prospective employer
8 solely for purposes related to the employee's status as a
9 current or former job applicant of such employer;

10 (2) information processed by an employer relating to
11 an employee who is acting in a professional capacity for
12 the employer, provided that such information is collected,
13 processed, or transferred solely for purposes related to
14 such employee's professional activities on behalf of the
15 employer;

16 (3) the business contact information of an employee,
17 including the employee's name, position or title, business
18 telephone number, business address, or business email
19 address that is provided to an employee by an employer who
20 is acting in a professional capacity, if such information
21 is collected, processed, or transferred solely for
22 purposes related to such employee's professional
23 activities on behalf of the employer;

24 (4) emergency contact information collected by an
25 employer that relates to an employee of that employer, if
26 such information is collected, processed, or transferred

1 solely for the purpose of having an emergency contact on
2 file for the employee and for processing or transferring
3 such information in case of an emergency; or

4 (5) information relating to an employee (or a spouse,
5 dependent, other covered family member, or beneficiary of
6 such employee) that is necessary for the employer to
7 collect, process, or transfer solely for the purpose of
8 administering benefits to which such employee (or spouse,
9 dependent, other covered family member, or beneficiary of
10 such employee) is entitled on the basis of the employee's
11 position with that employer.

12 "First party advertising or marketing" means advertising
13 or marketing conducted by a covered entity that collected
14 covered data from the individual linked or reasonably linkable
15 to that data through either direct communications with the
16 individual such as direct mail, email, or text message
17 communications, or advertising or marketing conducted entirely
18 within the first-party context, such as in a physical location
19 operated by or on behalf of such covered entity, or on a web
20 site or app operated by or on behalf of such covered entity.

21 "Genetic information" means any covered data, regardless
22 of its format, that concerns an individual's genetic
23 characteristics, including:

24 (1) raw sequence data that results from the sequencing
25 of the complete, or a portion of the, extracted
26 deoxyribonucleic acid (DNA) of an individual; or

(2) genotypic and phenotypic information that results from analyzing raw sequence data described in paragraph (1).

"Individual" means a natural person who is a resident of this State or present in this State.

"Knowledge" means

(1) with respect to a covered entity that is a covered high-impact social media company, the entity knew or should have known the individual was a covered minor;

(2) with respect to a covered entity or service provider that is a large data holder, and otherwise is not a covered high-impact social media company, that the covered entity knew or acted in willful disregard of the fact that the individual was a covered minor; and

(3) with respect to a covered entity or service provider that does not meet the requirements of paragraph (1) or (2), actual knowledge.

"Large data holder" means a covered entity or service provider that, in the most recent calendar year:

(1) had annual gross revenues of \$250,000,000 or more;
and

(2) collected, processed, or transferred the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to one or more individuals, excluding covered data collected and processed solely for the purpose of initiating, rendering,

1 billing for, finalizing, completing, or otherwise
2 collecting payment for a requested product or service; and
3 the sensitive covered data of more than 200,000
4 individuals or devices that identify or are linked or
5 reasonably linkable to one or more individuals.

6 "Large data holder" does not include any instance in which
7 the covered entity or service provider would qualify as a
8 large data holder solely on the basis of collecting or
9 processing personal email addresses, personal telephone
10 numbers, or log-in information of an individual or device to
11 allow the individual or device to log in to an account
12 administered by the covered entity or service provider.

13 "Market research" means the collection, processing, or
14 transfer of covered data as reasonably necessary and
15 proportionate to investigate the market for or marketing of
16 products, services, or ideas, where the covered data is not
17 integrated into any product or service, otherwise used to
18 contact any individual or individual's device, or used to
19 advertise or market to any individual or individual's device.

20 "Material" means, with respect to an act, practice, or
21 representation of a covered entity (including a representation
22 made by the covered entity in a privacy policy or similar
23 disclosure to individuals) involving the collection,
24 processing, or transfer of covered data, that such act,
25 practice, or representation is likely to affect a reasonable
26 individual's decision, conduct, or expectations regarding a

1 product or service or processing of personal data.

2 "Precise geolocation information" means information that
3 is derived from a device or technology that reveals the past or
4 present physical location of an individual or device that
5 identifies or is linked or reasonably linkable to one or more
6 individuals, with sufficient precision to identify street
7 level location information of an individual or device or the
8 location of an individual or device within a range of 1,850
9 feet or less. "Precise geolocation information" does not
10 include geolocation information identifiable or derived solely
11 from the visual content of a legally obtained image, including
12 the location of the device that captured such image.

13 "Process" means to conduct or direct any operation or set
14 of operations performed on covered data, including analyzing,
15 organizing, structuring, retaining, storing, using, or
16 otherwise handling covered data.

17 "Processing purpose" means a reason for which a covered
18 entity or service provider collects, processes, or transfers
19 covered data that is specific and granular enough for a
20 reasonable individual to understand the material facts of how
21 and why the covered entity or service provider collects,
22 processes, or transfers the covered data.

23 "Publicly available information" means any information
24 that a covered entity or service provider has a reasonable
25 basis to believe has been lawfully made available to the
26 general public from federal, State, or local government

1 records, if the covered entity collects, processes, and
2 transfers such information in accordance with any restrictions
3 or terms of use placed on the information by the relevant
4 government entity; widely distributed media; a website or
5 online service made available to all members of the public,
6 for free or for a fee, including where all members of the
7 public, for free or for a fee, can log in to the website or
8 online service; a disclosure that has been made to the general
9 public as required by federal, State, or local law; or the
10 visual observation of the physical presence of an individual
11 or a device in a public place, not including data collected by
12 a device in the individual's possession, provided that for
13 purposes of this paragraph, information from a website or
14 online service is not available to all members of the public if
15 the individual who made the information available via the
16 website or online service has restricted the information to a
17 specific audience. "Publicly available information" does not
18 include any obscene visual depiction (as defined in Section
19 1460 of title 18, United States Code), any inference made
20 exclusively from multiple independent sources of publicly
21 available information that reveals sensitive covered data with
22 respect to an individual, biometric information, publicly
23 available information that has been combined with covered
24 data, genetic information, unless otherwise made available by
25 the individual to whom the information pertains, or intimate
26 images known to have been created or shared without consent.

1 "Revenue" means, with respect to any covered entity or
2 service provider that is not organized to carry on business
3 for its own profit or that of its members, the gross receipts
4 the covered entity or service provider received, in whatever
5 form, from all sources, without subtracting any costs or
6 expenses; and includes contributions, gifts, grants, dues or
7 other assessments, income from investments, and proceeds from
8 the sale of real or personal property.

9 "Sensitive covered data" means the following types of
10 covered data:

11 (1) A government-issued identifier, such as a Social
12 Security number, passport number, or driver's license
13 number, that is not required by law to be displayed in
14 public.

15 (2) Any information that describes or reveals the
16 past, present, or future physical health, mental health,
17 disability, diagnosis, or health condition or treatment of
18 an individual.

19 (3) A financial account number, debit card number,
20 credit card number, or information that describes or
21 reveals the income level or bank account balances of an
22 individual, except that the last four digits of a debit or
23 credit card number shall not be deemed sensitive covered
24 data.

25 (4) Biometric information.

26 (5) Genetic information.

(6) Precise geolocation information.

(7) An individual's private communications such as voicemail, emails, texts, direct messages, or mail, or information identifying the parties to such communications, voice communications, video communications, and any information that pertains to the transmission of such communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call, unless the covered entity or a service provider acting on behalf of the covered entity is the sender or an intended recipient of the communication. Communications are not private for purposes of this clause if such communications are made from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that such employer may access such communications.

(8) Account or device log-in credentials, or security or access codes for an account or device.

(9) Information identifying the sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of such information.

(10) Calendar information, address book information, phone or text logs, photos, audio recordings, or videos, maintained for private use by an individual, regardless of

1 whether such information is stored on the individual's
2 device or is accessible from that device and is backed up
3 in a separate location. Such information is not sensitive
4 for purposes of this paragraph if such information is sent
5 from or to a device provided by an employer to an employee
6 insofar as such employer provides conspicuous notice that
7 it may access such information.

8 (11) A photograph, film, video recording, or other
9 similar medium that shows the naked or undergarment-clad
10 private area of an individual.

11 (12) Information revealing the video content requested
12 or selected by an individual collected by a covered entity
13 that is not a provider of a service described in paragraph
14 (4). This paragraph does not include covered data used
15 solely for transfers for independent video measurement.

16 (13) Information about an individual when the covered
17 entity or service provider has knowledge that the
18 individual is a covered minor.

19 (14) An individual's race, color, ethnicity, religion,
20 or union membership.

21 (15) Information identifying an individual's online
22 activities over time and across third party websites or
23 online services.

24 (16) Any other covered data collected, processed, or
25 transferred for the purpose of identifying the types of
26 covered data listed in paragraphs (1) through (15).

1 "Service provider" means a person or entity that collects,
2 processes, or transfers covered data on behalf of, and at the
3 direction of, a covered entity or a federal, State, tribal,
4 territorial, or local government entity; and receives covered
5 data from or on behalf of a covered entity or a federal, State,
6 tribal, territorial, or local government entity. A service
7 provider that receives service provider data from another
8 service provider as permitted under this Act shall be treated
9 as a service provider under this Act with respect to such data.

10 "Service provider data" means covered data that is
11 collected or processed by or has been transferred to a service
12 provider by or on behalf of a covered entity, a federal, State,
13 tribal, territorial, or local government entity, or another
14 service provider for the purpose of allowing the service
15 provider to whom such covered data is transferred to perform a
16 service or function on behalf of, and at the direction of, such
17 covered entity or federal, State, tribal, territorial, or
18 local government entity.

19 "Small business" means a covered entity or a service
20 provider that meets the following criteria for the period of
21 the 3 preceding calendar years (or for the period during which
22 the covered entity or service provider has been in existence
23 if such period is less than 3 years):

24 (1) the covered entity or service provider's average
25 annual gross revenues during the period did not exceed
26 \$41,000,000;

(2) the covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy; and

(3) is not a data broker.

"Substantial privacy risk" means the collection, processing, or transfer of covered data in a manner that may result in any reasonably foreseeable substantial physical injury, economic injury, highly offensive intrusion into the privacy expectations of a reasonable individual under the circumstances, or discrimination on the basis of race, color, religion, national origin, sex, or disability.

"Targeted advertising" means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier. "Targeted advertising" does not include advertising or marketing to an individual or an individual's device in response to the individual's specific request for

1 information or feedback; contextual advertising, which is when
2 an advertisement is displayed based on the content or nature
3 of the website or service in which the advertisement appears
4 and does not vary based on who is viewing the advertisement; or
5 processing covered data strictly necessary for the sole
6 purpose of measuring or reporting advertising or content,
7 performance, reach, or frequency, including independent
8 measurement.

9 "Third party" means:

10 (1) any person or entity, including a covered entity,
11 that:

12 (A) collects, processes, or transfers covered data
13 and is not a consumer-facing business with which the
14 individual linked or reasonably linkable to such
15 covered data expects and intends to interact; and

16 (B) is not a service provider with respect to such
17 data; and

18 (2) does not include a person or entity that collects
19 covered data from another entity if the 2 entities are
20 related by common ownership or corporate control, but only
21 if a reasonable consumer's reasonable expectation would be
22 that such entities share information.

23 "Third-party data" means covered data that has been
24 transferred to a third party.

25 "Transfer" means to disclose, release, disseminate, make
26 available, license, rent, or share covered data orally, in

1 writing, electronically, or by any other means.

2 "Unique identifier" means an identifier to the extent that
3 such identifier is reasonably linkable to an individual or
4 device that identifies or is linked or reasonably linkable to
5 one or more individuals, including a device identifier,
6 Internet Protocol address, cookie, beacon, pixel tag, mobile
7 ad identifier, or similar technology, customer number, unique
8 pseudonym, user alias, telephone number, or other form of
9 persistent or probabilistic identifier that is linked or
10 reasonably linkable to an individual or device; provided,
11 however, that "unique identifier" does not include an
12 identifier assigned by a covered entity for the specific and
13 exclusive purpose of giving effect to an individual's exercise
14 of affirmative express consent or opt-outs of the collection,
15 processing, and transfer of covered data pursuant to this Act
16 or otherwise limiting the collection, processing, or transfer
17 of such information.

18 "Widely distributed media" means information that is
19 available to the general public, including information from a
20 telephone book or online directory, a television, Internet, or
21 radio program, the news media, or an Internet site that is
22 available to the general public on an unrestricted basis, but
23 does not include an obscene visual depiction (as defined in 18
24 U.S.C. Sec. 1460).

25 Section 10. Data minimization.

1 (a) A covered entity may not collect, process, or transfer
2 covered data unless the collection, processing, or transfer is
3 limited to what is reasonably necessary and proportionate to:

4 (1) provide or maintain a specific product or service
5 requested by the individual to whom the data pertains; or

6 (2) effect a purpose permitted under subsection (b).

7 (b) A covered entity may collect, process, or transfer
8 covered data for any of the following purposes if the
9 collection, processing, or transfer is limited to what is
10 reasonably necessary and proportionate to such purpose:

11 (1) To initiate, manage, or complete a transaction or
12 fulfill an order for specific products or services
13 requested by an individual, including any associated
14 routine administrative, operational, and
15 account-servicing activity such as billing, shipping,
16 delivery, storage, and accounting.

17 (2) With respect to covered data previously collected
18 in accordance with this Act, notwithstanding this
19 exception:

20 (A) to process such data as necessary to perform
21 system maintenance or diagnostics;

22 (B) to develop, maintain, repair, or enhance a
23 product or service for which such data was collected;

24 (C) to conduct internal research or analytics to
25 improve a product or service for which such data was
26 collected;

(D) to perform inventory management or reasonable network management;

(E) to protect against spam; or

(F) to debug or repair errors that impair the functionality of a service or product for which such data was collected.

(3) To authenticate users of a product or service.

(4) To fulfill a product or service warranty.

(5) To prevent, detect, protect against, or respond to a security incident. For purposes of this paragraph, security is defined as network security and physical security and life safety, including an intrusion or trespass, medical alerts, fire alarms, and access control security.

(6) To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity targeted at or involving the covered entity or its services. For purposes of this paragraph, "illegal activity" means a violation of a federal, State, or local law punishable as a felony or misdemeanor that can directly harm.

(7) To comply with a legal obligation imposed by federal, tribal, local, or State law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider.

(8) To prevent an individual, or group of individuals, from suffering harm where the covered entity or service

1 provider believes in good faith that the individual, or
2 group of individuals, is at risk of death, serious
3 physical injury, or other serious health risk.

4 (9) To effectuate a product recall pursuant to federal
5 or State law.

6 (10) To conduct a public or peer-reviewed scientific,
7 historical, or statistical research project that:

8 (A) is in the public interest; and

9 (B) adheres to all relevant laws and regulations
10 governing such research, including regulations for the
11 protection of human subjects, or is excluded from
12 criteria of the institutional review board.

13 (11) To deliver a communication that is not an
14 advertisement to an individual, if the communication is
15 reasonably anticipated by the individual within the
16 context of the individual's interactions with the covered
17 entity.

18 (12) To deliver a communication at the direction of an
19 individual between such individual and one or more
20 individuals or entities.

21 (13) To transfer assets to a third party in the
22 context of a merger, acquisition, bankruptcy, or similar
23 transaction when the third party assumes control, in whole
24 or in part, of the covered entity's assets, only if the
25 covered entity, in a reasonable time prior to such
26 transfer, provides each affected individual with:

(A) a notice describing such transfer, including the name of the entity or entities receiving the individual's covered data and their privacy policies as described in Section 30; and

(B) a reasonable opportunity to withdraw any previously given consents in accordance with the requirements of affirmative express consent under this Act related to the individual's covered data and a reasonable opportunity to request the deletion of the individual's covered data, as described in Section 35.

(14) To ensure the data security and integrity of covered data, as described in Section 55.

(15) to support or promote participation by individuals in civic engagement activities and democratic governance, including voting, petitioning, engaging with government proceedings, providing indigent legal aid services, and unionizing.

(16) With respect to covered data previously collected in accordance with this Act, to process such data as necessary to provide first party advertising or marketing of products or services provided by the covered entity for individuals who are not-covered minors.

(17) With respect to covered data previously collected in accordance with this Act, provided such collection, processing, and transferring complies with subsection

(c) of Section 40, to provide targeted advertising.

(c) A covered entity or service provider may not engage in deceptive advertising or marketing with respect to a product or service offered to an individual.

(d) Nothing in this Act shall be construed to limit or diminish First Amendment freedoms guaranteed under the Constitution.

Section 15. Loyalty duties. Notwithstanding Section 10 and unless an exception applies, with respect to covered data, a covered entity or service provider may not:

(1) collect, process, or transfer a Social Security number, except when necessary to facilitate an extension of credit, authentication, fraud and identity fraud detection and prevention, the payment or collection of taxes, the enforcement of a contract between parties, or the prevention, investigation, or prosecution of fraud or illegal activity, or as otherwise required by federal, State, or local law;

(2) collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data pertains, or is strictly necessary to effect a purpose enumerated in paragraphs (1) through (12) and (14) through (15) of subsection (b) of Section 10;

(3) transfer an individual's sensitive covered data to a third party, unless:

(A) the transfer is made pursuant to the affirmative express consent of the individual;

(B) the transfer is necessary to comply with a legal obligation imposed by federal, State, tribal, or local law, or to establish, exercise, or defend legal claims;

(C) the transfer is necessary to prevent an individual from imminent injury where the covered entity believes in good faith that the individual is at risk of death, serious physical injury, or serious health risk;

(D) in the case of the transfer of a password, the transfer is necessary to use a designated password manager or is to a covered entity for the exclusive purpose of identifying passwords that are being re-used across sites or accounts;

(E) in the case of the transfer of genetic information, the transfer is necessary to perform a medical diagnosis or medical treatment specifically requested by an individual, or to conduct medical research in accordance with conditions of paragraph (10) of subsection (b) of Section 10; or

(F) to transfer assets in the manner described in paragraph (13) of subsection (b) of Section 10; or

(4) in the case of a provider of broadcast television service, cable service, satellite service, streaming media service, or other video programming service described in Section 713(h)(2) of the Communications Act of 1934 (47 U.S.C. 613(h)(2)), transfer to an unaffiliated third party covered data that reveals the video content or services requested or selected by an individual from such service, except with the affirmative express consent of the individual or pursuant to one of the permissible purposes enumerated in paragraphs (1) through (15) of subsection (b) of Section 10.

Section 20. Privacy by design.

(a) A covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data and that:

(1) consider applicable federal and State laws, rules, or regulations related to covered data the covered entity or service provider collects, processes, or transfers;

(2) identify, assess, and mitigate privacy risks related to covered minors to result in reasonably necessary and proportionate residual risk to covered minors;

(3) mitigate privacy risks, including substantial

1 privacy risks, related to the products and services of the
2 covered entity or the service provider, including in the
3 design, development, and implementation of such products
4 and services, taking into account the role of the covered
5 entity or service provider and the information available
6 to it; and

7 (4) implement reasonable training and safeguards
8 within the covered entity and service provider to promote
9 compliance with all privacy laws applicable to covered
10 data the covered entity collects, processes, or transfers
11 or covered data the service provider collects, processes,
12 or transfers on behalf of the covered entity and mitigate
13 privacy risks, including substantial privacy risks, taking
14 into account the role of the covered entity or service
15 provider and the information available to it.

16 (b) The policies, practices, and procedures established by
17 a covered entity and a service provider under subsection (a),
18 shall correspond with, as applicable:

19 (1) the size of the covered entity or the service
20 provider and the nature, scope, and complexity of the
21 activities engaged in by the covered entity or service
22 provider, including whether the covered entity or service
23 provider is a large data holder, nonprofit organization,
24 small business, third party, or data broker, taking into
25 account the role of the covered entity or service provider
26 and the information available to it;

(2) the sensitivity of the covered data collected, processed, or transferred by the covered entity or service provider;

(3) the volume of covered data collected, processed, or transferred by the covered entity or service provider;

(4) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity or service provider relates; and

(5) the cost of implementing such policies, practices, and procedures in relation to the risks and nature of the covered data.

Section 25. Prohibition on retaliation against an individual for exercise of rights.

(a) A covered entity may not retaliate against an individual for exercising any of the rights guaranteed by the Act, or any regulations promulgated under this Act, or for refusing to agree to collection or processing of covered data for a separate product or service, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services.

(b) Nothing in subsection (a) may be construed to:

(1) prohibit the relation of the price of a service or the level of service provided to an individual to the provision, by the individual, of financial information

1 that is necessarily collected and processed only for the
2 purpose of initiating, rendering, billing for, or
3 collecting payment for a service or product requested by
4 the individual;

5 (2) prohibit a covered entity from offering a
6 different price, rate, level, quality or selection of
7 goods or services to an individual, including offering
8 goods or services for no fee, if the offering is in
9 connection with an individual's voluntary participation in
10 a bona fide loyalty, rewards, premium features, discount
11 or club card program, provided that the covered entity may
12 not transfer covered data to a third party as part of such
13 a program unless:

14 (A) the transfer is reasonably necessary to enable
15 the third party to provide a benefit to which the
16 individual is entitled;

17 (B) the transfer of covered data to third parties
18 is clearly disclosed in the terms of the program; and

19 (C) the third party uses the covered data only for
20 purposes of facilitating such a benefit to which the
21 individual is entitled and does not retain or
22 otherwise use or disclose the covered data for any
23 other purpose, including for the delivery of targeted
24 advertisements.

25 (3) require a covered entity to provide a bona fide
26 loyalty program that would require the covered entity to

1 collect, process, or transfer covered data that the
2 covered entity otherwise would not collect, process, or
3 transfer;

4 (4) prohibit a covered entity from offering a
5 financial incentive or other consideration to an
6 individual for participation in market research;

7 (5) prohibit a covered entity from offering different
8 types of pricing or functionalities with respect to a
9 product or service based on an individual's exercise of a
10 right under paragraph (3) of subsection (a) of Section 35;
11 or

12 (6) prohibit a covered entity from declining to
13 provide a product or service insofar as the collection and
14 processing of covered data is strictly necessary for such
15 product or service.

16 (c) Notwithstanding the provisions in this subsection, no
17 covered entity may offer different types of pricing that are
18 unjust, unreasonable, coercive, or usurious in nature.

19 Section 30. Transparency.

20 (a) Each covered entity and service provider shall make
21 publicly available, in a clear, conspicuous, not misleading,
22 and easy-to-read and readily accessible manner, a privacy
23 policy that provides a detailed and accurate representation of
24 the data collection, processing, and transfer activities of
25 the covered entity. The policy must be provided in a manner

that is reasonably accessible to and usable by individuals with disabilities. The policy shall be made available to the public in each covered language in which the covered entity or service provider provides a product or service that is subject to the privacy policy; or carries out activities related to such product or service. The policy must include, at a minimum, the following:

(1) The identity and the contact information of:

(A) the covered entity or service provider to which the privacy policy applies (including the covered entity's or service provider's points of contact and generic electronic mail addresses, as applicable for privacy and data security inquiries); and

(B) any other entity within the same corporate structure as the covered entity or service provider to which covered data is transferred by the covered entity.

(2) The categories of covered data the covered entity or service provider collects or processes.

(3) The processing purposes for each category of covered data the covered entity or service provider collects or processes.

(4) Whether the covered entity or service provider transfers covered data and, if so, each category of service provider and third party to which the covered

1 entity or service provider transfers covered data, the
2 name of each data broker to which the covered entity or
3 service provider transfers covered data, and the purposes
4 for which such data is transferred to such categories of
5 service providers and third parties or third-party
6 collecting entities, except for a transfer to a
7 governmental entity pursuant to a court order or law that
8 prohibits the covered entity or service provider from
9 disclosing such transfer.

10 (5) The length of time the covered entity or service
11 provider intends to retain each category of covered data,
12 including sensitive covered data, or, if it is not
13 possible to identify that timeframe, the criteria used to
14 determine the length of time the covered entity or service
15 provider intends to retain categories of covered data.

16 (6) A prominent description of how an individual can
17 exercise the rights described in this Act.

18 (7) A general description of the covered entity's or
19 service provider's data security practices.

20 (8) The effective date of the privacy policy.

21 (b) If a covered entity makes a material change to its
22 privacy policy or practices, the covered entity shall notify
23 each individual affected by such material change before
24 implementing the material change with respect to any
25 prospectively collected covered data and, except as provided
26 in paragraphs (1) through (15) of subsection (b) of Section

1 10, provide a reasonable opportunity for each individual to
2 withdraw consent to any further materially different
3 collection, processing, or transfer of previously collected
4 covered data under the changed policy. The covered entity
5 shall take all reasonable electronic measures to provide
6 direct notification regarding material changes to the privacy
7 policy to each affected individual, in each covered language
8 in which the privacy policy is made available, and taking into
9 account available technology and the nature of the
10 relationship. Nothing in this Section may be construed to
11 affect the requirements for covered entities under Section 15
12 or 25.

13 (c) Each large data holder shall retain copies of previous
14 versions of its privacy policy for at least 10 years beginning
15 after the date of enactment of this Act and publish them on its
16 website. Such large data holder shall make publicly available,
17 in a clear, conspicuous, and readily accessible manner, a log
18 describing the date and nature of each material change to its
19 privacy policy over the past 10 years. The descriptions shall
20 be sufficient for a reasonable individual to understand the
21 material effect of each material change. The obligations in
22 this paragraph shall not apply to any previous versions of a
23 large data holder's privacy policy, or any material changes to
24 such policy, that precede the date of enactment of this Act.

25 (d) In addition to the privacy policy required under
26 subsection (a), a large data holder that is a covered entity

1 shall provide a short-form notice of its covered data
2 practices in a manner that is:

3 (1) concise, clear, conspicuous, and not misleading;

4 (2) readily accessible to the individual, based on
5 what is reasonably anticipated within the context of the
6 relationship between the individual and the large data
7 holder;

8 (3) inclusive of an overview of individual rights and
9 disclosures to reasonably draw attention to data practices
10 that may reasonably be unexpected to a reasonable person
11 or that involve sensitive covered data; and

12 (4) no more than 500 words in length.

13 Section 35. Individual data rights.

14 (a) In accordance with subsections (b) and (c), a covered
15 entity shall provide an individual, after receiving a verified
16 request from the individual, with the right to:

17 (1) access:

18 (A) in a human-readable format that a reasonable
19 individual can understand and download from the
20 Internet, the covered data (except covered data in a
21 back-up or archival system) of the individual making
22 the request that is collected, processed, or
23 transferred by the covered entity or any service
24 provider of the covered entity within the 24 months
25 preceding the request;

(B) the categories of any third party, if applicable, and an option for consumers to obtain the names of any such third party as well as and the categories of any service providers to whom the covered entity has transferred for consideration the covered data of the individual, as well as the categories of sources from which the covered data was collected; and

(C) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider;

(2) correct any verifiable substantial inaccuracy or substantially incomplete information with respect to the covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the corrected information;

(3) delete covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the individual's deletion request; and

(4) to the extent technically feasible, export to the individual or directly to another entity the covered data

1 of the individual that is processed by the covered entity,
2 including inferences linked or reasonably linkable to the
3 individual but not including other derived data, without
4 licensing restrictions that limit such transfers in:

5 (A) a human-readable format that a reasonable
6 individual can understand and download from the
7 Internet; and

8 (B) a portable, structured, interoperable, and
9 machine-readable format.

10 (b) A covered entity may not condition, effectively
11 condition, attempt to condition, or attempt to effectively
12 condition the exercise of a right described in subsection (a)
13 through:

14 (1) the use of any false, fictitious, fraudulent, or
15 materially misleading statement or representation; or

16 (2) the design, modification, or manipulation of any
17 user interface with the purpose or substantial effect of
18 obscuring, subverting, or impairing a reasonable
19 individual's autonomy, decision-making, or choice to
20 exercise such right.

21 (c) Subject to subsections (d) and (e), each request under
22 subsection (a) shall be completed by any:

23 (1) large data holder within 45 days after the request
24 from an individual, unless it is demonstrably
25 impracticable or impracticably costly to verify such
26 individual;

(2) covered entity that is not a large data holder within 60 days after the request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual; or

(3) a response period set forth in this subsection may be extended once by 45 additional days when reasonably necessary, considering the complexity and number of the individual's requests, so long as the covered entity informs the individual of any such extension within the initial 45-day response period, together with the reason for the extension.

(d) A covered entity shall provide an individual with the opportunity to exercise each of the rights described in subsection (a); and with respect to the first 2 times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right free of charge; and any time beyond the initial 2 times described in subparagraph (A), may allow the individual to exercise such right for a reasonable fee for each request.

(e) A covered entity may not permit an individual to exercise a right described in subsection (a), in whole or in part, if the covered entity:

(1) cannot reasonably verify that the individual making the request to exercise the right is the individual whose covered data is the subject of the request or an individual authorized to make such a request on the

1 individual's behalf;

2 (2) reasonably believes that the request is made to
3 interfere with a contract between the covered entity and
4 another individual;

5 (3) determines that the exercise of the right would
6 require access to or correction of another individual's
7 sensitive covered data;

8 (4) reasonably believes that the exercise of the right
9 would require the covered entity to engage in an unfair or
10 deceptive practice under Section 5 of the Federal Trade
11 Commission Act (15 U.S.C. 45); or

12 (5) reasonably believes that the request is made to
13 further fraud, support criminal activity, or the exercise
14 of the right presents a data security threat.

15 (f) If a covered entity cannot reasonably verify that a
16 request to exercise a right described in subsection (a) is
17 made by the individual whose covered data is the subject of the
18 request (or an individual authorized to make such a request on
19 the individual's behalf), the covered entity:

20 (1) may request that the individual making the request
21 to exercise the right provide any additional information
22 necessary for the sole purpose of verifying the identity
23 of the individual; and

24 (2) may not process or transfer such additional
25 information for any other purpose.

26 (g) A covered entity may decline, with adequate

1 explanation to the individual, to comply with a request to
2 exercise a right described in subsection (a), in whole or in
3 part, that would:

4 (1) require the covered entity to retain any covered
5 data collected for a single, one-time transaction, if such
6 covered data is not processed or transferred by the
7 covered entity for any purpose other than completing such
8 transaction;

9 (2) be demonstrably impracticable or prohibitively
10 costly to comply with, and the covered entity shall
11 provide a description to the requester detailing the
12 inability to comply with the request;

13 (3) require the covered entity to attempt to
14 re-identify de-identified data;

15 (4) require the covered entity to maintain covered
16 data in an identifiable form or collect, retain, or access
17 any data in order to be capable of associating a verified
18 individual request with covered data of such individual;

19 (5) result in the release of trade secrets or other
20 privileged or confidential business information;

21 (6) require the covered entity to correct any covered
22 data that cannot be reasonably verified as being
23 inaccurate or incomplete;

24 (7) interfere with law enforcement, judicial
25 proceedings, investigations, or reasonable efforts to
26 guard against, detect, prevent, or investigate fraudulent,

1 malicious, or unlawful activity, or enforce valid
2 contracts;

3 (8) violate federal or State law or the rights and
4 freedoms of another individual, including under the
5 Constitution of the United States;

6 (9) prevent a covered entity from being able to
7 maintain a confidential record of deletion requests,
8 maintained solely for the purpose of preventing covered
9 data of an individual from being recollected after the
10 individual submitted a deletion request and requested that
11 the covered entity no longer collect, process, or transfer
12 such data; or

13 (10) with respect to requests for deletion:

14 (A) unreasonably interfere with the provision of
15 products or services by the covered entity to another
16 person it currently serves;

17 (B) delete covered data that relates to a public
18 figure and for which the requesting individual has no
19 reasonable expectation of privacy;

20 (C) delete covered data reasonably necessary to
21 perform a contract between the covered entity and the
22 individual;

23 (D) delete covered data that the covered entity
24 needs to retain in order to comply with professional
25 ethical obligations;

26 (E) delete covered data that the covered entity

1 reasonably believes may be evidence of unlawful
2 activity or an abuse of the covered entity's products
3 or services; or

4 (F) for private elementary and secondary schools
5 as defined by State law and private institutions of
6 higher education as defined by Title I of the Higher
7 Education Act of 1965, delete covered data that would
8 unreasonably interfere with the provision of education
9 services by or the ordinary operation of the school or
10 institution.

11 (h) In a circumstance that would allow a denial, a covered
12 entity shall partially comply with the remainder of the
13 request if it is possible and not unduly burdensome to do so.

14 (i) For purposes of paragraph (2) of subsection (g), the
15 receipt of a large number of verified requests, on its own, may
16 not be considered to render compliance with a request
17 demonstrably impracticable.

18 (j) A covered entity shall facilitate the ability of
19 individuals to make requests under this Section in any covered
20 language in which the covered entity provides a product or
21 service. The mechanisms by which a covered entity enables
22 individuals to make requests under this Section shall be
23 readily accessible and usable by individuals with
24 disabilities.

25 Section 40. Right to consent.

1 (a) A covered entity shall provide an individual with a
2 clear and conspicuous, easy-to-execute means to withdraw any
3 affirmative express consent previously provided by the
4 individual that is as easy to execute by a reasonable
5 individual as the means to provide consent, with respect to
6 the processing or transfer of the covered data of the
7 individual.

8 (b) A covered entity may not transfer or direct the
9 transfer of the covered data of an individual to a third party
10 without obtaining the individual's affirmative express
11 consent:

12 (1) A covered entity need not allow an individual to
13 opt out of the collection, processing, or transfer of
14 covered data made pursuant to the exceptions in paragraphs
15 (1) through (15) of subsection (b) of Section 10.

16 (c) A covered entity or service provider that directly
17 delivers a targeted advertisement shall prior to engaging in
18 targeted advertising to an individual gather the affirmative
19 express consent of the individual.

20 (d) A covered entity may not condition, effectively
21 condition, attempt to condition, or attempt to effectively
22 condition the exercise of any individual right under this
23 Section through:

24 (1) the use of any false, fictitious, fraudulent, or
25 materially misleading statement or representation; or

26 (2) the design, modification, or manipulation of any

1 user interface with the purpose or substantial effect of
2 obscuring, subverting, or impairing a reasonable
3 individual's autonomy, decision-making, or choice to
4 exercise any such right.

5 Section 45. Data protections for children and minors.

6 (a) A covered entity may not engage in targeted
7 advertising to any individual if the covered entity has
8 knowledge that the individual is a covered minor.

9 (b) A covered entity may not transfer or direct the
10 transfer of the covered data of a covered minor to a third
11 party if the covered entity has knowledge that the individual
12 is a covered minor; and has not obtained affirmative express
13 consent from the covered minor or the covered minor's parent
14 or guardian; provided that a covered entity or service
15 provider may collect, process, or transfer covered data of an
16 individual the covered entity or service provider knows is
17 under the age of 18 solely in order to submit information
18 relating to child victimization to law enforcement or to the
19 nonprofit, national resource center and clearinghouse
20 congressionally designated to provide assistance to victims,
21 families, child-serving professionals, and the general public
22 on missing and exploited children issues.

23 Section 50. Civil rights.

24 (a) A covered entity or a service provider may not

1 collect, process, or transfer covered data in a manner that
2 discriminates in or otherwise makes unavailable the equal
3 enjoyment of goods or services on the basis of race, color,
4 religion, national origin, sex, or disability. This does not
5 apply to:

6 (1) the collection, processing, or transfer of covered
7 data for the purpose of:

8 (A) a covered entity's or a service provider's
9 self-testing to prevent or mitigate unlawful
10 discrimination; or

11 (B) diversifying an applicant, participant, or
12 customer pool; or

13 (2) any private club or group not open to the public,
14 as described in Section 201(e) of the Civil Rights Act of
15 1964 (42 U.S.C. 2000a(e)).

16 Section 55. Data security and protection of covered data.

17 (a) A covered entity or service provider shall establish,
18 implement, and maintain reasonable administrative, technical,
19 and physical data security practices and procedures to protect
20 and secure covered data against unauthorized access and
21 acquisition. The practices shall be appropriate to:

22 (1) the size and complexity of the covered entity or
23 service provider;

24 (2) the nature and scope of the covered entity or the
25 service provider's collecting, processing, or transferring

1 of covered data;

2 (3) the volume and nature of the covered data
3 collected, processed, or transferred by the covered entity
4 or service provider;

5 (4) the sensitivity of the covered data collected,
6 processed, or transferred;

7 (5) the current state of the art (and limitations
8 thereof) in administrative, technical, and physical
9 safeguards for protecting such covered data; and

10 (6) the cost of available tools to improve security
11 and reduce vulnerabilities to unauthorized access and
12 acquisition of such covered data in relation to the risks
13 and nature of the covered data.

14 (b) The data security practices of the covered entity and
15 of the service provider required under subsection (a) shall
16 include, for each respective entity's own system or systems,
17 at a minimum, the following practices:

18 (1) Identifying and assessing any material internal
19 and external risk to, and vulnerability in, the security
20 of each system maintained by the covered entity that
21 collects, processes, or transfers covered data, or service
22 provider that collects, processes, or transfers covered
23 data on behalf of the covered entity, including
24 unauthorized access to or risks to such covered data,
25 human vulnerabilities, access rights, and the use of
26 service providers. With respect to large data holders,

1 such activities shall include a plan to receive and
2 reasonably respond to unsolicited reports of
3 vulnerabilities by any entity or individual and by
4 performing a reasonable investigation of such reports.

5 (2) Taking preventive and corrective action designed
6 to mitigate reasonably foreseeable risks or
7 vulnerabilities to covered data identified by the covered
8 entity or service provider, consistent with the nature of
9 such risk or vulnerability and the entity's role in
10 collecting, processing, or transferring the data. Such
11 action may include implementing administrative, technical,
12 or physical safeguards or changes to data security
13 practices or the architecture, installation, or
14 implementation of network or operating software, among
15 other actions.

16 (3) Disposing of covered data in accordance with a
17 retention schedule that shall require the deletion of
18 covered data when such data is required to be deleted by
19 law or is no longer necessary for the purpose for which the
20 data was collected, processed, or transferred, unless an
21 individual has provided affirmative express consent to
22 such retention. Such disposal shall include destroying,
23 permanently erasing, or otherwise modifying the covered
24 data to make such data permanently unreadable or
25 indecipherable and unrecoverable to ensure ongoing
26 compliance with this Section. Service providers shall

1 establish practices to delete or return covered data to a
2 covered entity as requested at the end of the provision of
3 services unless retention of the covered data is required
4 by law, consistent with this Act.

5 (4) Training each employee with access to covered data
6 on how to safeguard covered data and updating such
7 training as necessary.

8 (5) Designating an officer, employee, or employees to
9 maintain and implement such practices.

10 (6) Implementing procedures to detect, respond to, or
11 recover from security incidents, including breaches.

12 Section 60. Small business protections. A small business:

13 (1) is exempt from compliance with paragraph (4) of
14 subsection (a) of Section 35; and

15 (2) at the small business' sole discretion, may comply
16 with paragraph (2) of subsection (a) of Section 35 by,
17 after receiving a verified request from an individual to
18 correct covered data of the individual under such Section,
19 deleting such covered data in its entirety instead of
20 making the requested correction.

21 Section 65. Executive responsibility.

22 (a) Beginning one year after the date of enactment of this
23 Act, an executive officer of a large data holder shall
24 annually certify, in good faith, to the Attorney General that

1 the entity maintains:

2 (1) internal controls reasonably designed to comply
3 with this Act; and

4 (2) internal reporting structures to ensure that such
5 certifying executive officer is involved in and
6 responsible for the decisions that impact the compliance
7 by the large data holder with this Act.

8 (b) A certification submitted under subsection (a) shall
9 be based on a review of the effectiveness of the internal
10 controls and reporting structures of the large data holder
11 that is conducted by the certifying executive officer not more
12 than 90 days before the submission of the certification. A
13 certification submitted under subsection (a) is made in good
14 faith if the certifying officer had, after a reasonable
15 investigation, reasonable ground to believe and did believe,
16 at the time that certification was submitted, that the
17 statements therein were true and that there was no omission to
18 state a material fact required to be stated therein or
19 necessary to make the statements therein not misleading.

20 (c) A covered entity or service provider that is not a
21 small business shall designate one or more qualified employees
22 as privacy officers; and one or more qualified employees as
23 data security officers.

24 (1) An employee who is designated by a covered entity
25 or a service provider as a privacy officer or a data
26 security officer shall, at a minimum:

(A) implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this Act; and

(B) facilitate the covered entity or service provider's ongoing compliance with this Act.

(2) A large data holder shall designate at least one the officers described in subsection (c) to report directly to the highest official at the large data holder a privacy protection officer who shall, in addition to requirements in paragraph (1), either directly or through a supervised designee or designees:

(A) establish processes to periodically review and update the privacy and security policies, practices, and procedures of the large data holder, as necessary;

(B) conduct biennial and comprehensive audits to ensure the policies, practices, and procedures of the large data holder ensure the large data holder is in compliance with this Act and ensure such audits are accessible to the Attorney General upon request;

(C) develop a program to educate and train employees about compliance requirements of this Act;

(D) maintain updated, accurate, clear, and understandable records of all material privacy and data security practices undertaken by the large data holder; and

(E) serve as the point of contact between the large data holder and enforcement authorities.

(d) Not later than one year after the date of enactment of this Act and biennially thereafter, each covered entity that is not a small business shall conduct a privacy impact assessment. Such assessment shall weigh the benefits of the covered entity's covered data collecting, processing, and transfer practices that may cause a substantial privacy risk against the potential material adverse consequences of such practices to individual privacy. The covered entity shall make a summary of such privacy impact assessment publicly available in a place that is easily accessible to individuals. The privacy impact assessment shall:

(1) be reasonable and appropriate in scope given:

(A) the nature of the covered data collected, processed, and transferred by the covered entity;

(B) the volume of the covered data collected, processed, and transferred by the covered entity; and

(C) the potential risks posed to the privacy of individuals by the collecting, processing, and transfer of covered data by the covered entity;

(2) be documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under paragraph (1);

(3) include additional information required by regulations issued by the Attorney General;

(4) upon request, make such impact assessments available to the Attorney General; and

(5) if the covered entity is a large data holder, be approved by the privacy protection officer designated in this Section, as applicable.

Section 70. Service providers and third parties.

(a) A service provider:

(1) shall adhere to the instructions of a covered entity and only collect, process, and transfer service provider data to the extent necessary and proportionate to provide a service requested by the covered entity, as set out in the contract required by subsection (b), and this paragraph does not require a service provider to collect, process, or transfer covered data if the service provider would not otherwise do so;

(2) may not collect, process, or transfer service provider data if the service provider has actual knowledge that a covered entity violated this Act with respect to such data;

(3) shall assist a covered entity in responding to a request made by an individual under Section 35 or 40, by either:

(A) providing appropriate technical and organizational measures, taking into account the nature of the processing and the information

reasonably available to the service provider, for the covered entity to comply with such request for service provider data; or

(B) fulfilling a request by a covered entity to execute an individual rights request that the covered entity has determined should be complied with, by either:

(i) complying with the request pursuant to the covered entity's instructions; or

(ii) providing written verification to the covered entity that it does not hold covered data related to the request, that complying with the request would be inconsistent with its legal obligations, or that the request falls within an exception to Section 35 or 40;

(4) may engage another service provider for purposes of processing service provider data on behalf of a covered entity only after providing that covered entity with notice and pursuant to a written contract that requires such other service provider to satisfy the obligations of the service provider with respect to such service provider data, including that the other service provider be treated as a service provider under this Act;

(5) shall, at the covered entity's direction, delete or return all covered data to the covered entity as requested at the end of the provision of services, unless

1 retention of the covered data is required by law;

2 (6) shall develop, implement, and maintain reasonable
3 administrative, technical, and physical safeguards that
4 are designed to protect the security and confidentiality
5 of covered data the service provider processes consistent
6 with Section 55; and

7 (7) shall allow and cooperate with, reasonable
8 assessments by the covered entity or the covered entity's
9 designated assessor; alternatively, the service provider
10 may arrange for a qualified and independent assessor to
11 conduct an assessment of the service provider's policies
12 and technical and organizational measures in support of
13 the obligations under this Act using an appropriate and
14 accepted control standard or framework and assessment
15 procedure for such assessments. The service provider shall
16 provide a report of such assessment to the covered entity
17 upon request.

18 (b) A person or entity may only act as a service provider
19 pursuant to a written contract between the covered entity and
20 the service provider, or a written contract between one
21 service provider and a second service provider as described
22 under paragraph (4) of subsection (a), if the contract:

23 (1) sets forth the data processing procedures of the
24 service provider with respect to collection, processing,
25 or transfer performed on behalf of the covered entity or
26 service provider;

(2) clearly sets forth:

(A) instructions for collecting, processing, or transferring data;

(B) the nature and purpose of collecting, processing, or transferring;

(C) the type of data subject to collecting, processing, or transferring;

(D) the duration of processing; and

(E) the rights and obligations of both parties,

including a method by which the service provider shall notify the covered entity of material changes to its privacy practices;

(3) does not relieve a covered entity or a service provider of any requirement or liability imposed on such covered entity or service provider under this Act; and

(4) prohibits:

(A) collecting, processing, or transferring covered data in contravention to subsection (a); and

(B) combining service provider data with covered data which the service provider receives from or on behalf of another person or persons or collects from the interaction of the service provider with an individual, provided that such combining is not necessary to effectuate a purpose described in paragraphs (1) through (15) of subsection (b) of Section 10 and is otherwise permitted under the

contract required by this subsection.

(5) Each service provider shall retain copies of previous contracts entered into in compliance with this Section with each covered entity to which it provides requested products or services.

(c) Relationship between covered entities and service providers:

(1) Determining whether a person is acting as a covered entity or service provider with respect to a specific processing of covered data is a fact-based determination that depends upon the context in which such data is processed.

(2) A person that is not limited in its processing of covered data pursuant to the instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and not a service provider with respect to a specific processing of covered data. A service provider that continues to adhere to the instructions of a covered entity with respect to a specific processing of covered data remains a service provider. If a service provider begins, alone or jointly with others, determining the purposes and means of the processing of covered data, it is a covered entity and not a service provider with respect to the processing of such data.

(3) A covered entity that transfers covered data to a service provider or a service provider that transfers

1 covered data to a covered entity or another service
2 provider, in compliance with the requirements of this Act,
3 is not liable for a violation of this Act by the service
4 provider or covered entity to whom such covered data was
5 transferred, if at the time of transferring such covered
6 data, the covered entity or service provider did not have
7 actual knowledge that the service provider or covered
8 entity would violate this Act.

9 (4) A covered entity or service provider that receives
10 covered data in compliance with the requirements of this
11 Act is not in violation of this Act as a result of a
12 violation by a covered entity or service provider from
13 which such data was received.

14 (d) A third party:

15 (1) shall not process third-party data for a
16 processing purpose other than, in the case of sensitive
17 covered data, the processing purpose for which the
18 individual gave affirmative express consent or to effect a
19 purpose enumerated in paragraphs (1), (3), or (5) of
20 subsection (b) of Section 10 and, in the case of
21 non-sensitive data, the processing purpose for which the
22 covered entity made a disclosure pursuant to paragraph (4)
23 of subsection (1) of Section 30;

24 (2) for purposes of paragraph (1), may reasonably rely
25 on representations made by the covered entity that
26 transferred the third party data if the third party

1 conducts reasonable due diligence on the representations
2 of the covered entity and finds those representations to
3 be credible; and

4 (3) shall enter into and comply with all provisions of
5 the contract required under subsection (e).

6 (e) A covered entity that transfers covered data to a
7 third party shall enter into a written contract with such
8 third party that:

9 (1) identifies the specific purposes for which the
10 covered data is being made available to third party;

11 (2) specifies that the covered entity is transferring
12 the covered data to the third party solely for the
13 specific purposes set forth in the contract and that the
14 third party may only use the covered data for such
15 specific purposes;

16 (3) requires the third party to comply with all
17 applicable provisions of and regulations promulgated under
18 this Act with respect to the covered data that the covered
19 entity transfers to the third party and must provide the
20 same level of privacy and security protection for the
21 covered data as required by covered entities under this
22 Act.

23 (f) A covered entity or service provider shall exercise
24 reasonable due diligence in:

25 (1) selecting a service provider; and

26 (2) deciding to transfer covered data to a third

1 party.

2 (g) Solely for the purposes of this Section, the
3 requirements for service providers to contract with, assist,
4 and follow the instructions of covered entities shall be read
5 to include requirements to contract with, assist, and follow
6 the instructions of a government entity if the service
7 provider is providing a service to a government entity.

8 Section 75. Enforcement. The Attorney General, State's
9 Attorney, or a municipality's attorney may bring a civil
10 action in the name of the State, or as parens patriae on behalf
11 of the residents of the State, against any covered entity or
12 service provider that violated this Act to:

13 (1) enjoin such act or practice;

14 (2) enforce compliance with this Act or such
15 regulation;

16 (3) obtain damages, civil penalties, restitution, or
17 other compensation on behalf of the residents of such
18 State; or

19 (4) obtain reasonable attorneys' fees and other
20 litigation costs reasonably incurred.

21 Section 80. Enforcement by persons.

22 (a) Any person or class of persons subject to a violation
23 of this Act or a regulation promulgated under this Act by a
24 covered entity or service provider may bring a civil action

1 against such entity in any court of competent jurisdiction.

2 (b) In a civil action brought under paragraph (a) in which
3 a plaintiff prevails, the court may award the plaintiff:

- 4 (1) an amount equal to the sum of any compensatory,
5 liquidated, or punitive damages;
- 6 (2) injunctive relief;
- 7 (3) declaratory relief; and
- 8 (4) reasonable attorney's fees and litigation costs.

9 (c) This Section shall not apply to any claim against a
10 small business.

11 Section 85. Rulemaking.

12 (a) The Attorney General may adopt rules for the purposes
13 of carrying out this Act, including, but not limited to, the
14 following areas:

15 (1) adjusting the monetary thresholds in January of
16 every odd-numbered year to reflect any increase in the
17 Consumer Price Index, and the data collected thresholds in
18 the definition of "large data holder" and "small business"
19 as appropriate;

20 (2) further defining "precise geolocation
21 information," such as where the size defined is not
22 sufficient to protect individual privacy in sparsely
23 populated areas, or when the covered data is used for
24 normal operational purposes, such as billing;

25 (3) updating or adding categories to the definition of

1 "sensitive covered data" any other type of covered data
2 that may require a similar level of protection as the
3 types of covered data listed in the definition of
4 "sensitive covered data" as a result of any new method of
5 collecting, processing, or transferring covered data;

6 (4) further defining and adding to the permissible
7 purposes under subsection (b) of Section 10 for which
8 covered entities and service providers may use covered
9 data, as long as such purposes are consistent with the
10 reasonable expectations of individuals;

11 (5) further defining what constitutes reasonable
12 policies, practices, and procedures under Section 20;

13 (6) establishing processes by which covered entities
14 are to comply with the provisions of Section 35. Such
15 regulations may take into consideration:

16 (A) the size of, and the nature, scope, and
17 complexity of the activities engaged in by the covered
18 entity, including whether the covered entity is a
19 large data holder, nonprofit organization, small
20 business, third party, or data broker;

21 (B) the sensitivity of covered data collected,
22 processed, or transferred by the covered entity;

23 (C) the volume of covered data collected,
24 processed, or transferred by the covered entity;

25 (D) the number of individuals and devices to which
26 the covered data collected, processed, or transferred

1 by the covered entity relates; and

2 (E) standards for ensuring the deletion of covered
3 data under this Act where appropriate;

4 (7) establishing rules and procedures to further the
5 purposes of Section 35 and to facilitate an individual's
6 or the individual's authorized agent's ability to delete
7 covered data, correct inaccurate covered data, or obtain
8 covered data, with the goal of minimizing the
9 administrative burden on individuals, taking into account
10 available technology, security concerns, and the burden on
11 the covered entity, to govern a covered entity's
12 determination that a request for information received by
13 from an individual is a verifiable consumer request,
14 including treating a request submitted through a
15 password-protected account maintained by the individual
16 with the covered entity while the individual is logged
17 into the account as a verifiable request and providing a
18 mechanism for an individual who does not maintain an
19 account with the covered entity to request information
20 through the covered entity's authentication of the
21 individual's identity;

22 (8) establishing additional permissive exceptions
23 necessary to protect the rights of individuals, prevent
24 unjust or unreasonable outcomes from the exercise of
25 access, correction, deletion, or portability rights, or as
26 otherwise necessary to fulfill the purposes of this

1 Section. In establishing such exceptions, the Attorney
2 General should consider any relevant changes in
3 technology, means for protecting privacy and other rights,
4 and beneficial uses of covered data by covered entities;

5 (9) establishing how often, and under what
6 circumstances, an individual may request a correction
7 pursuant to Section 35;

8 (10) requiring covered entities obligated to conduct
9 impact assessments under subsection (d) of Sections 65 to
10 establish a process to ensure that audits are thorough and
11 independent;

12 (11) requiring additional information necessary for
13 compliance with the impact assessment required under
14 subsection (d) of Sections 65; and

15 (12) setting compliance requirements for service
16 providers and third parties under Section 70.

17 Section 97. Severability. The provisions of this Act are
18 severable under Section 1.31 of the Statute on Statutes.

19 Section 99. Effective date. This Act takes effect 180 days
20 after becoming law.